目　录

§1 整　　数

整数是这样一些数：…，-2，-1，0，1，2，…．数论的很大一部分内容就是研究整数的性质．整数通常只用来提供数据（如3个苹果，32元，$17x^2+9$等），人们并不考虑它们的性质．3有多少个因子？32是否为素数？17能不能写为两个整数的平方和？我们在给苹果、钞票或x^2计数时，这些问题都是无关紧要的．但是，整数是数学中非常基本的内容，人们认为它们本身就值得加以研究．

从本节开始，除非另有说明，小写字母总表示整数．整数的加法、减法、乘法和除法的通常性质以及整数的有序性，我们认为大家已经知道，并将随时应用．本节中，我们还要用到整数的一个重要性质，由于它不象某些性质（如乘法结合律）那样经常地明确表出，因此你也许还未认真地加以注意．此性质叫做*最小整数原理*：一个下有界的非空整数集合总包含有它的最小元．也可以说，一个上有界的非空整数集合总包含有它的最大元．

当且仅当存在一个整数d使$ad=b$时，我们称a *整除* b，记为$a|b$．例如，$2|6$，$12|60$，$17|17$，$-5|50$，$8|-24$．如a不能整除b，我们写作$a\nmid b$．例如，$4\nmid 2$，$3\nmid 4$．

【练习1】　哪些整数整除零？

【练习2】　证明：若$a|b$，$b|c$，则$a|c$．

为了说明整除具有怎样的性质，我们证明下列引理：

引理1　若$d|a$，$d|b$，则$d|(a+b)$．

证明 根据整除的定义，我们知道存在整数 q 和 r，使

$$dq=a,\ dr=b.$$

因此
$$a+b=d(q+r).$$

故再由定义，$d|(a+b)$.

引理 2 若 $d|a$，则对任何整数 c，$d|ca$.

引理 3 若 $d|a_1$，$d|a_2$，$\cdots$，$d|a_n$，则对任何整数 c_1，c_2，$\cdots$，c_n，有 $d|(c_1a_1+c_2a_2+\cdots+c_na_n)$.

这两个引理的证明是很容易的.

【练习 3】 证明引理 2 和引理 3.

作为引理 3 的应用，我们知道，若 d 整除一个方程一端的所有项，则它也整除此方程另一端. 因此，若 $a+b=c$，且 $d|a$，$d|c$，则 $d|b$. 又若

$$3x+81y+6z+363=w,$$

则 $3|w$，因为 3 整除该方程左端所有项（记住：所有小写字母，包括 x，y，z，w 在内，除非另有说明，均表示整数）. 类似地，若

$$3x^2+15xy+5y^2=0,$$

则 $3|5y^2$，$5|3x^2$.

本节的其余部分将用以研究最大公因子及其性质，这些性质我们以后要经常用到. 我们称 d 是 a 和 b 的**最大公因子**（记为 $d=(a,\ b)$），当且仅当：

(i) $d|a$，$d|b$；

(ii) 若 $c|a$，$c|b$，则 $c\leqslant d$.

条件(i)说明，d 是 a 和 b 的公因子；条件(ii)说明，它是这种因子中最大的一个. 注意，若 a 和 b 不同时为零，那么 a 和 b 的公因子集合是以 a，b，$-a$ 和 $-b$ 中最大者为其上界的整数集. 因此，根据整数的良序原理，该集合有最大元，故 a 和

b 的最大公因子存在，而且是唯一的. 注意，$(0, 0)$没有定义；而如(a, b)有意义，则它是正数. 事实上，必成立$(a, b)\geqslant 1$，因为对任何 a 和 b，$1|a$，$1|b$.

【练习 4】 $(4, 14)$，$(5, 15)$，$(6, 16)$各是什么？

【练习 5】 设 n 为任意正整数，$(n, 1)$是什么？$(n, 0)$是什么？

【练习 6】 若 d 为正整数，(d, nd)是什么？

作为使用最大公因子的定义的一个练习，我们将证明下列定理，它在以后要常用到.

定理 1 若$(a, b)=d$，则$(a/d, b/d)=1$.

证明 设 $c=(a/d, b/d)$. 我们需证 $c=1$. 为此，我们证明，$c\leqslant 1$ 且 $c\geqslant 1$. 由于 c 是两个整数的最大公因子，我们已注意到，每个最大公因子都大于或等于 1，故得后一不等式. 为了说明 $c\leqslant 1$，我们利用 $c|(a/d)$ 和 $c|(b/d)$，即知存在 q 和 r，使 $cq=a/d$，$cr=b/d$，或$(cd)q=a$，$(cd)r=b$. 这两个式子表明，cd 是 a 和 b 的一个公因子，因此它不大于 a 和 b 的最大公因子 d，故有 $cd\leqslant d$. 又因 d 是正数，可得 $c\leqslant 1$. 因此，$c=1$，乃所欲证.

若$(a, b)=1$，我们就称 a 和 b *互素*. 其道理在学习因子分解唯一性这一节时即可明白.

当(a, b)较小时，常可用观察法看出(a, b). 当 a 和 b 很大时，就不大容易看出了. 如：$(31415926, 5358979)$是什么？现在我们介绍一种求最大公因子的有效方法：欧几里得(Euclid)算法. 这种算法在证明我们后面需要的一些定理时也是有用的.

定理 2(除法算式) 给定正整数 a 和 b，$b\neq 0$，存在唯一的整数 q 和 r(其中 $0\leqslant r<b$)，使

$$a=bq+r.$$

证明 如将 $a=bq+r$ 写为

$$\frac{a}{b}=q+\frac{r}{b},$$

我们就可看到，此定理只是说明了我们用 b 除 a 具体是怎么做的罢了：求出一个商 q 和一个余数 r. 我们可将此写得更为正式一些. 考虑整数 $a-bt$ 构成的集合 S，其中 $t=0, \pm 1, \pm 2, \cdots$. 因为 S 中有非负元(如 a, $a+b$ 等)，由最小整数原理，我们知道 S 有一个最小的非负元，把它叫做 r，并设 q 是相应的 t 值，则 $a-bq=r$，且 $r\geqslant 0$. 为了完成定理的证明，我们尚需证 $r<b$. 假若不然，则有 $r=b+r_1$，且 $r_1\geqslant 0$. 因而，

$$r_1=r-b=a-bq-b=a-b(q+1).$$

这就说明，r_1 在集合 S 中. 但

$$0\leqslant r_1=r-b<r,$$

这是不可能的，因为 r 是集合 S 中的最小非负元.

上述作法给出了 q 和 r，剩下来要证明，它们是唯一确定的. 假定我们找到了 q, r 和 q_1, r_1，使

$$a=bq+r=bq_1+r_1,$$

其中 $0\leqslant r<b$, $0\leqslant r_1<b$. 两式相减，我们有

(1) $$0=b(q-q_1)+(r-r_1).$$

由于 b 整除此式左端以及右端第一项，它也整除右端另一项：$b\mid(r-r_1)$. 但因 $0\leqslant r<b$, $0\leqslant r_1<b$，我们有

$$-b<r-r_1<b.$$

$-b$ 和 b 之间的 b 的倍数只有零，因而 $r-r_1=0$. 由(1)又得 $q-q_1=0$. 因此，定理中的数 q 和 r 是唯一确定的.

虽然此定理只是对正整数 a 和 b 而言的(因为它最经常

地用于正整数)，但在证明过程中，我们始终不必要求 a 是正数. 此外，若 b 为负数，只要将 $0\leqslant r<b$ 换成 $0\leqslant r<-b$，定理也一样成立. 请你将上述证明再读一遍，进而验证这一点.

【练习 7】 当 $a=75$, $b=24$ 时，q 和 r 是多少？当 $a=75$, $b=25$ 时，q 和 r 又是多少？

定理 2 连同下一引理即可推出欧几里得算法.

引理 4 若 $a=bq+r$，则 $(a, b)=(b, r)$.

证明 设 $d=(a,b)$. 我们知道，因 $d|a$, $d|b$，由 $a=bq+r$ 即可得 $d|r$，故 d 是 b 和 r 的一个公因子. 假定 c 是 b 和 r 的任一公因子，我们知 $c|b$, $c|r$，由 $a=bq+r$，可得 $c|a$. 因而 c 是 a 和 b 的公因子，故 $c\leqslant d$. d 满足最大公因子定义中的两个条件，故我们有 $d=(b, r)$.

【练习 8】 当 $a=16$, $b=6$ 时，验证此引理的正确性.

根据引理 4，我们对 a 和 b 用除法算式，可得

$$(a, b)=(b, r);$$

最大公因子相同，但右端括号中有了更小的数. 我们可继续对 b 和 r 用除法算式而得更小的数，但最大公因子仍然相同. 除法算式用了相当次数后，这些数终将变得较小，以致我们能用观察法看出最大公因子来. 例如，我们来算一算 $(5767, 4453)$. 用除法算式，我们有

$$5767=4453\cdot1+1314.$$

由引理 4，我们知 $(5767, 4453)=(4453, 1314)$. 除非你非常善于观察，否则要看出其最大公因子，这两个整数仍嫌太大. 我们再次相除：

$$4453=1314\cdot3+511.$$

现在我们知道，$(5767, 4453)=(1314, 511)$. 我们继续相除：

$$1314=511\cdot2+292,$$

$$511=292\cdot 1+219,$$
$$292=219\cdot 1+73,$$
$$219=73\cdot 3.$$

上面一系列余数中，最后一个为零(必然如此，因为一个非负整数的递降序列决不能无限地写下去)，而由引理 4，我们就知道，

$$(5767,\ 4453)=(4453,\ 1314)=\cdots=(219,\ 73)$$
$$=(73,\ 0)=73.$$

将上面这一特殊例子中所用的方法正式写出来，就是欧几里得算法.

定理 3(欧几里得算法) 若 a 和 b 为正整数，$b\neq 0$，且

$$a=bq+r,\quad 0\leqslant r<b,$$
$$b=rq_1+r_1,\quad 0\leqslant r_1<r,$$
$$r=r_1q_2+r_2,\quad 0\leqslant r_2<r_1,$$
$$\cdots\qquad\qquad\cdots$$
$$r_{k-1}=r_kq_{k+1}+r_{k+1},\quad 0\leqslant r_{k+1}<r_k,$$

则对足够大的 k，比如 $k=t$，我们有

$$r_{t-1}=r_tq_{t+1},$$

且 $(a,\ b)=r_t$.

证明 下列非负整数序列必有终点:

$$b>r>r_1>r_2>\cdots.$$

所以，这些余数中最后必出现零，假定就是 $r_{t+1}=0$，那么

$$r_{t-1}=r_tq_{t+1}.$$

反复应用引理 4，可得

$$(a,\ b)=(b,\ r)=(r,\ r_1)=(r_1,\ r_2)=\cdots$$
$$=(r_{t-1},\ r_t)=r_t.$$

若 a 和 b 中有一个为负数，我们可利用

$$(a, b)=(-a, b)=(a, -b)=(-a, -b).$$

【练习 9】 计算(299, 247)和(578, 442).

下面是欧几里得算法的一个推论，以后要多次用到.

定理 4 若$(a, b)=d$, 则有x和y使$ax+by=d$.

证明 其想法是：将欧几里得算法倒推上去. 以(5767, 4453)=73 这一计算为例. 算法中倒数第二行给出

$$73=292-219.$$

我们用它前面一行将 73 表为 511 和 292 的一个组合:

$$73=292-(511-292)=2\cdot 292-511.$$

再用更前面一行来消去 292:

$$73=2(1314-511\cdot 2)-511=2\cdot 1314-5\cdot 511.$$

依此类推:

$$73=2\cdot 1314-5(4453-3\cdot 1314)=17\cdot 1314-5\cdot 4453.$$

最后，我们可把 1314 用 4453 和 5767 表出，从而求得所要之表示式:

$$73=17(5767-4453)-5\cdot 4453=17\cdot 5767-22\cdot 4453.$$

一般地，我们有

$$d=(a, b)=r_t=r_{t-2}-r_{t-1}q_t,$$

它将d表成了r_{t-1}和r_{t-2}的具有整系数的一个组合. 从算法中在其前面的一行

$$r_{t-3}=r_{t-2}q_{t-1}+r_{t-1},$$

我们可得 $$d=r_{t-2}-(r_{t-3}-r_{t-2}q_{t-1})q_t,$$

它将d表成了r_{t-2}和r_{t-3}的具有整系数的一个组合:

$$d=(q_{t-1}q_t+1)r_{t-2}-q_tr_{t-3}.$$

然后我们可用

$$r_{t-4}=r_{t-3}q_{t-2}+r_{t-2}$$

消去r_{t-2}, 得

$$d=(\text{整数})\cdot r_{t-3}+(\text{整数})\cdot r_{t-2},$$

若我们依此继续做下去，最后将求得 x 和 y，使

$$d=ax+by.$$

【练习 10】 求出 $299x+247y=13$ 的一组解.

定理 4 有许多应用，现在我们介绍后面将要用到的两个.

定理 5 若 $d|ab$, $(d, a)=1$, 则 $d|b$.

证明 由于 d 和 a 互素，由定理 4 我们知，存在整数 x 和 y，使

$$dx+ay=1.$$

两端乘以 b，我们有

$$d(bx)+(ab)y=b.$$

上式左端第一项当然可被 d 整除，由于 $d|ab$，d 也整除左端第二项，因此 d 也整除右端，这就是我们所要证明的.

注意，在定理 5 中，若 d 与 a 不互素，那么结论未必成立例如，$6|8\cdot 9$，但 $6\nmid 8$, $6\nmid 9$.

定理 6 令 $(a, b)=d$，且设 $c|a$, $c|b$，则 $c|d$.

证明 此定理说起来就是，两个整数的任一公因子也是它们的最大公因子的因子. 证明非常简短. 我们知，存在整数 x 和 y，使

$$ax+by=d.$$

由于 c 整除此式左端的两项，c 也整除右端.

习 题

1. 计算：(a) (314, 159)；　　(b) (3141, 1592)；
   (c) (4144, 7696)；　　(d) (10,001, 100,083).
2. 证明：若 $a|b$, $b|a$，则 $a=b$ 或 $a=-b$.
3. 证明：若 $a|b$, $a>0$，则 $(a, b)=a$.
4. 证明：$((a, b), b)=(a, b)$.

5. 说明“$a>b$ 蕴涵 $a\nmid b$”这一命题不真.

6. (a) 证明：对所有 $n>0$，有 $(n,n+1)=1$;

   (b) 当 $n>0$ 时，$(n, n+2)$ 可取什么值?

   (c) 当 $n>0$ 时，$(n, n+k)$ 可取什么值?

7. 若 $N=n_1n_2\cdots n_k+1$，证明：对于 $i=1, 2, \cdots, k$，有 $(n_i, N)=1$.

8. 证明：若 $(a, b)=1$，$c|a$，则 $(c, b)=1$.

9. 求 x 和 y，使

   (a) $314x+159y=1$;　　(b) $3141x+1592y=1$;

   (c) $4144x+7696y=592$;　　(d) $10001x+100083y=73$.

10. (a) 证明：当且仅当 $(k, n)=1$ 时，成立 $(k, n+k)=1$;

    (b) “当且仅当 $(k,n)=d$ 时，成立 $(k,n+k)=d$”，这一说法对不对?

    (c) “当且仅当 $(k, n)=d$ 时，对所有整数 r，有 $(k, n+rk)=d$”，这一说法对不对?

11. (a) 证明：$(299, 247)=13$;

    (b) 求出 $299x+247y=13$ 的两组解;

    (c) 求出 $299x+247y=52$ 的两组解.

12. (a) 若 $x^2+ax+b=0$ 有一整数根，证明此根整除 b;

    (b) 若 $x^2+ax+b=0$ 有一有理数根，证明此根实际上是一整数.

13. 证明：若 $a|b$，$c|d$，则 $ac|bd$.

14. 证明：若 $d|a$，$d|b$，则 $d^2|ab$.

15. 证明：若 $c|ab$，$(c, a)=d$，则 $c|db$.

16. 证明：若 d 为奇数，$d|(a+b)$，$d|(a-b)$，则 $d|(a, b)$.

17. 证明：“若 $a\nmid b$，则 $(a, b)=1$”未必成立.

18. 证明：由 $p|(10a-b)$ 和 $p|(10c-d)$，可得 $p|(ad-bc)$.

19. 证明：对所有 $n>0$，有 $6|(n^3-n)$.

20. (a) 证明：若对某一 m 有 $10|(3^m+1)$，则对所有 $n>0$，有 $10|(3^{m+4n}+1)$;

    (b) 当 m 是怎样的数时，有 $10|(3^m+1)$?

§2 因子分解的唯一性

本节的目的是介绍素数，它是数论研究的主要对象之一；同时还要证明正整数因子分解的唯一性定理，它对于以后的内容也是十分重要的. 本节中，小写字母总是代表正整数.

大于1、且除了1和它自身外没有其它正因子的整数称为素数. 大于1而又不是素数的整数叫做合数. 这样，2，3，5，7等都是素数，4，6，8，9等都是合数. 还存在着很大的素数，如

170,141,183,460,469,231,731,687,303,715, 884,105,727

就是一个素数. 合数显然可以任意大. 注意，我们称1既非素数，也非合数. 虽然1除了1和它自身外，没有其它正因子，但如把它包括在素数内，有些定理(特别是因子分解唯一性定理)会变得非常麻烦. 我们将把1称为单位元. 这样，正整数集合就被分成了三类：素数、合数和单位元.

【练习1】 偶素数有多少个？末位数为5的素数有多少个？

我们的目标是要证明，每一正整数都能写为素数之积，而且这种写法是唯一的. 若两个乘积只是其因子的次序不相同，我们将不把它们看作为不同的分解式. 因此，

$$2^2\cdot3\cdot7,\ 2\cdot3\cdot7\cdot2,\ 7\cdot3\cdot2\cdot2$$

中每一个我们都看作是84的同一分解式. 这样，整个正整数系统就可通过素数的乘法建立起来. 以下，起先的两个引理

将要表明，任一正整数均可写为素数的乘积，接着我们再证明这种表示式的唯一性.

引理1 每个整数 n, $n>1$, 均可被一素数整除.

证明 若 n 是素数，则引理已经得证，因为 n 整除自身. 反之，假定 n 为合数，那么，根据定义，n 除了 1 和自身外，还有另一因子，假定 d_1 就是那个因子，则对某个 n_1，有 $n=d_1n_1$，且由于 $d_1\neq 1$ 或 n，可得 $1<n_1<n$.（事实上，有 $n_1\leqslant\frac{n}{2}$，但我们只需要用到它小于 n 这一点.）若 n_1 为素数，则 $n_1|n$，我们找到了 n 的一个素因子，引理也就得证. 但若 n_1 也为合数，则对于某整数 n_2，有 $n_1=d_2n_2$，且 $1<n_2<n_1$. 若 n_2 为素数，那么我们不必再证明下去了：n_2 是一个素数，且 $n_2|n$（因为 $n_2|n_1$, $n_1|n$）. 若 n_2 不是素数，即它为合数（注意，n_2 大于 1），就有 $n_2=d_3n_3$，且 $1<n_3<n_2$. 如此继续下去：在 n, n_1, n_2, n_3, … 这些数中，终将出现一个素数，这是因为

$$n>n_1>n_2>n_3>n_4>\cdots,$$

而每个 n_i 均大于 1，递减正整数列不可能无限继续下去. 终将出现一个素数，将它称为 n_k，则因

$$n_k|n_{k-1},\quad n_{k-1}|n_{k-2},\quad \cdots,\quad n_1|n,$$

可推出 $n_k|n$.

利用归纳法原理的第二种形式（见附录一），可以更有效地证得引理 1. 由观察知，引理 1 对 $n=2$ 成立. 假定它对所有 $n\leqslant k$ 成立，那么，要末 $k+1$ 是素数，此时论证即可结束；要末 $k+1$ 被某 k_1 整除，且 $k_1\leqslant k$. 但根据归纳法假设，k_1 被一个素数整除，该素数也就整除 $k+1$. 论证同样可以结束. 这种证法在本质上与第一种证法相同，只是归纳法原理代替了前面用到的“如此继续下去”一语.

利用引理1，并借助于类似于此引理的证明中用到的论据，我们可以证明，对每一正整数，至少有一种方式将它写为素数的乘积。

引理2 每个整数 n, $n>1$, 均可写为素数的乘积.

证明 由引理1我们知，存在一个素数 p_1 使 $p_1|n$，即 $n=p_1n_1$，其中 $1\leqslant n_1<n$. 若 $n_1=1$，那么论证即可结束，$n=p_1$ 就是 n 的素因子乘积的一个表示式. 若 $n_1>1$，则同样由引理1，存在一素数整除 n_1，即 $n_1=p_2n_2$，其中 p_2 为素数，且 $1\leqslant n_2<n_1$. 若 $n_2=1$，论证同样可以结束：$n=p_1p_2$ 已经写成了素数的乘积；但若 $n_2>1$，由引理1再次得到 $n_2=p_3n_3$，p_3 为一素数，且 $1\leqslant n_3<n_2$. 若 $n_3=1$，论证可以结束，否则我们继续进行下去. 我们迟早会得到一个 n_i，它等于1，这是因为：$n>n_1>n_2>\cdots$，而每一 n_i 都是正数，这样一个序列不会无限继续下去. 对某个 k，我们将有 $n_k=1$. 这样，$n=p_1p_2\cdots p_k$ 就是欲求的 n 的素数乘积表示式. 注意，同一素数在此乘积中可能会出现好几次.

【练习2】(选做) 使用归纳法作出引理2的证明.

【练习3】 写出72和480的素数分解式.

在证明每一正整数只有一种素数分解式以前，我们先证一个古老而优美的定理：

定理1(欧几里得) 存在着无限多个素数.

证明 假定不然，那么素数只有有限多个，将它们记为 p_1, p_2, $\cdots$, p_r. 考虑整数

$$n=p_1p_2\cdots p_r+1. \tag{1}$$

由引理1，我们知 n 可被一个素数整除，又因为只有有限多个素数，故此素数必为 p_1, p_2, $\cdots$, p_r 中之一，假定就是 p_k. 那么，由于 $p_k|n$, $p_k|p_1p_2\cdots p_r$，即 p_k 整除(1)中两项，因此它也

整除(1)中余下一项，即 $p_k|1$. 这是荒谬的：没有素数能整除 1，因为任何素数都大于 1. 这一矛盾说明，我们开始时的假设是不对的. 既然素数不可能只有有限多个，就应有无限多个.

这是一个很强的定理. 我们在实际上能够判明的素数却只有有限多个，目前知道的最大素数是 $2^{11213}-1$[注]，而且小于此数的素数我们也没有全搞清楚.（小于 10^8 的所有素数的表已经造出，超出此数很多的素数表却还没有.）素数 $2^{11213}-1$ 比 10^8 要大得多：它有 3376 位. 虽然 $2^{11213}-1$ 是一个很大的数，比它大的整数仍有无限多个，而比它小的整数却只有有限多个. 因此，虽然我们只能说出有限多个素数，但我们可以相信，无论我们发现了多少素数，总还存在一个素数需要我们去寻找. 在高速计算机发展起来以前，人们知道的最大素数就是本节开头写出的那个 39 位数，相对地说它还是很小的. 因此，如果你不求助于机器而着手寻找一个比 $2^{11213}-1$ 还要大的素数的话，将要耗费大量的时间——至少要好几个世纪.

在证明因子分解唯一性定理以前，我们还要离题谈谈另一件事，说明一下如何制造一张素数表.

引理 3 若 n 是合数，则它有一因子 d 满足 $1<d\leqslant n^{1/2}$.

证明 由于 n 是合数，故存在整数 d_1 和 d_2 使 $n=d_1d_2$，其中 $1<d_1<n$，$1<d_2<n$. 如 d_1 和 d_2 均大于 $n^{1/2}$，则 $n=d_1d_2>n^{1/2}n^{1/2}=n$，这是不可能的，因此 d_1 和 d_2 中必有一个小于或等于 $n^{1/2}$.

引理 4 若 n 是合数，则它必有一个素因子小于或等于

[注] 现在我们知道的最大素数是 $2^{19937}-1$，它有 6002 位（参见王元“谈谈素数”一书的介绍，第 8 页，1978 年 11 月上海教育出版社出版）.——译校者注

$n^{1/2}$.

证明 由引理3我们知道，n有一个因子，称它为d，满足$1<d\leqslant n^{1/2}$. 由引理1我们知道，d具有一个素因子p. 由于$p\leqslant d\leqslant n^{1/2}$，引理得证.

引理4为寻找素数的古代方法，即有名的厄拉多塞(Eratosthenes)筛法提供了基础. 写下1到N各数，在2上打一圆圈，划去所有其它的2的倍数. 第一个未打圆圈又未划去的数是3，将它打圈，划去它的所有倍数. 现在既非打圈又未划去的第一个数是5，它就是3后面的第一个素数. 再将它打圈，并划去它的所有倍数，依此继续，一直到所有小于或等于$N^{1/2}$的各数都打了圆圈或划去为止. 那么，表中打了圆圈的及未划去的那些数正好就是小于或等于N的素数. 在说明为什么会如此之前，让我们先看一例. 取$N=81$；此时$N^{1/2}=9$. 经筛选我们得

②	~~14~~	~~26~~	~~38~~	~~50~~	~~62~~	~~74~~
③	~~15~~	~~27~~	~~39~~	~~51~~	~~63~~	~~75~~
~~4~~	~~16~~	~~28~~	~~40~~	~~52~~	~~64~~	~~76~~
⑤	17	29	41	53	~~65~~	~~77~~
~~6~~	~~18~~	~~30~~	~~42~~	~~54~~	~~66~~	~~78~~
⑦	19	31	43	~~55~~	67	79
~~8~~	~~20~~	~~32~~	~~44~~	~~56~~	~~68~~	~~80~~
~~9~~	~~21~~	~~33~~	~~45~~	~~57~~	~~69~~	~~81~~
~~10~~	~~22~~	~~34~~	~~46~~	~~58~~	~~70~~	
11	23	~~35~~	47	59	71	
~~12~~	~~24~~	~~36~~	~~48~~	~~60~~	~~72~~	
13	~~25~~	37	~~49~~	61	73	

划去2, 3, 5, 7的倍数后，我们就发现了小于81的所有素数. 类似地，要求出小于10,000的所有素数，我们只需划去小于100的25个素数的倍数即可.

为了得知这一方法是正确的,应注意,打了圆圈的任一数必为素数. 这是因为,若它为合数,它就有一个比它自身要小的素因子,因此它应已被划去. 另外,任一未被划去的数也是素数. 假如这样一个数不是素数, 那么, 由引理 4, 它就有一个小于或等于 $N^{1/2}$ 的素因子. 但我们已经划去了全部具有小于或等于 $N^{1/2}$ 的素因子的数. 因此,未划去的数和打了圆圈的数均为素数. 在划去的数中, 每一个都有一个异于自身的素因子,故均为合数.

要是你企图列出大量的数并开始筛选的话,不要忘记,这种事以前就已经有人试过. 十九世纪, 一位名叫居利克(Kulik)的奥地利天文学家造出了一面巨大的筛子, 它包括了 10^8 以内的所有整数. 这一工作断断续续花去了他 20 年时间,却未得到人们的重视,连他留下手稿的那个图书馆也竟将手稿的一部分失落了, 丢失的部分就包括了从 12, 642, 600 到 22, 852, 800 间的那些整数.

下一引理给出的结果使我们有可能去证明因子分解的唯一性. 在本节余下部分,在未另作说明之前,字母 p 和 q 将专门用来表示素数.

引理 5 若 $p|ab$, 则 $p|a$ 或 $p|b$.

证明 由于 p 是素数, 它仅有的正因子为 1 和 p, 因此, $(p, a)=p$ 或 $(p, a)=1$. 在第一种情况下, $p|a$, 论证即可结束; 在第二种情况下, §1 定理 5 告诉我们, $p|b$, 引理也就得证.

【练习 4】 若 $p|a_1a_2\cdots a_k$, 你能得出什么结论?

【练习 5】 用归纳法证明练习 4 的结论.

引理 6 若 $q_1, q_2, \cdots, q_n$ 均为素数, $p|q_1q_2\cdots q_n$, 则对某 k, 有 $p=q_k$.

证明 由练习 5 我们知，对某 k，有 $p|q_k$. 由于 p 和 q_k 均为素数，故 $p=q_k$. (q_k 仅有的正因子为 1 和 q_k，但 p 不为 1.)

定理 2 (因子分解唯一性定理) 任一正整数都能用一种方式也只能用一种方式写成素数的乘积.

证明 提醒一下，我们已约定，仅仅是因子次序不同的所有因子分解式都被看作是完全相同的.

我们已由引理 2 得知，任一整数 $n(n>1)$ 均可写为素数的乘积. 因此要完成定理的证明，我们只要说明，n 不能有两种这样的表示式. 即若

(2) $$n=p_1p_2\cdots p_m \quad 和 \quad n=q_1q_2\cdots q_r,$$

则我们必须证明，每个乘积中都出现同样一些素数，且各素数出现次数也一样(虽然次序可能不一样). 也就是说，我们要证明，整数 $p_1, p_2, \cdots, p_m$ 只不过是整数 $q_1, q_2, \cdots, q_r$ 的一个重新排列而已. 由(2)我们看到，由于 $p_1|n$，$p_1|q_1q_2\cdots q_r$. 由引理 6 可得，对某一 i，有 $p_1=q_i$. 如我们用此公因子去除

$$p_1p_2\cdots p_m=q_1q_2\cdots q_r,$$

我们得

(3) $$p_2p_3\cdots p_m=q_1q_2\cdots q_{i-1}q_{i+1}\cdots q_r.$$

由于 p_2 整除此式左端，故它也整除其右端. 同样应用引理 6 可得，对某一 $j(j=1, 2, \cdots, i-1, i+1, \cdots, n)$，有 $p_2=q_j$. 从(3)两端约去这一因子，并将这种做法继续进行下去，最终我们会发现，每一 p 都是一个 q. (在所有的 p 被约去以前，q 不可能全部用完，因为要是那样的话，我们就会得到素数的一个乘积等于 1，这是不可能的.) 如果将所有 p 和所有 q 的地位对调，重复上述论证，我们看到每一 q 也是一个 p. 这样，$p_1, p_2, \cdots, p_m$ 各数就是 $q_1, q_2, \cdots, q_r$ 的一个重新排列，两种因子分解的方式至多只是因子次序不同而已.

素数分解式的唯一性也可用归纳法给予有效的证明，当然证明思想并没有什么不同．由观察知，定理对 $n=2$ 为真．假定它对 $n\leqslant k$ 为真，并设 $k+1$ 有两种表示式：

$$k+1=p_1p_2\cdots p_m=q_1q_2\cdots q_r.$$

和前一证法一样，对某一 i，有 $p_1=q_i$，故

$$p_2p_3\cdots p_m=q_1q_2\cdots q_{i-1}q_{i+1}\cdots q_r.$$

但此数小于或等于 k，由归纳法假设，它的素数分解式是唯一的，因此整数 $p_2, p_3, \cdots, p_m$ 是 $q_1, q_2, \cdots, q_{i-1}, q_{i+1}, \cdots, q_r$ 的一个重新排列，又由 $p_1=q_i$，证明也就完成了．

由于你与正整数打了长期交道（你还记得不懂 $2+3$ 等于几的情况吗？），你可能认为因子分解唯一性定理没有多少意思；你甚至会以为这是不证自明的事．下述例子将用来说明，它并非象你所想的那样显而易见：我们来构造一种数系，对于它因子分解唯一性定理就不成立．考虑整数 1, 5, 9, 13, 17, …, 即所有形为 $4n+1$ 的整数（$n=0, 1, \cdots$）．如果一个元素在此集合中除 1 和自身外，没有别的因子，我们就称它为“素数”．例如，21 是“素数”，而 $25=5\cdot5$ 就不是“素数”．

【练习 6】 此集合中，小于 100 的数有哪些是“素数”？

用证明引理 1 和引理 2 的同一方法，我们可证，此集合中每个数都有一个“素因子”，每个数都可写为“素数”的乘积．（请你查看一下引理 1 和引理 2 的证明，看看是否有什么字需要修改．）但举一例即可表明，此集合中的一个整数的“素数”分解式并不总是唯一的：

$$693=21\cdot33=9\cdot77,$$

而 9, 21, 33, 77 等均为“素数”．

由因子分解唯一性定理可得，每一正整数都恰有一种方式写成下列形式：

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},$$

其中 $e_i\geqslant 1$, $i=1, 2, \cdots, k$, 每个 p_i 都是素数, 且 $i\neq j$ 时, $p_i\neq p_j$. 我们将这一表示式叫做 n 的素数幂分解式, 且每当我们写出如上的素数幂分解式时, 若未另加说明, 就应作这样的理解: 所有指数均为正, 各素数互不相同. 表 A 给出了小于 10^5 且不能被 2 和 5 整除的所有 n 的最小素因子. 借助此表, 任何 $n\leqslant 10^5$ 的素数幂分解式都易求得. 例如, 取 8001, 它显然不能被 2 或 5 整除, 表 A 给出它的最小素因子为 3, 那么, $8001/3=2667$. 该表又表明, 3 也是 2667 的因子: $2667/3=889$. 同样查表可知 $7\mid 889$. 最后, $889/7=127$, 它是素数. 这样,

$$8001=3^2\cdot 7\cdot 127.$$

【练习 7】 7950 的素数幂分解式是什么?

在结束本节前, 我们还注意到, 整数的素数分解式提供了不用欧几里得算法而求出最大公因子的另一方法. 例如, 考虑 $n=120=2^3\cdot 3\cdot 5$ 和 $m=252=2^2\cdot 3^2\cdot 7$. 我们看到, 2^2 整除 m 和 n, 但 2 的更高次幂都不是 m 和 n 的公因子. 又, 3 整除 m 和 n, 3 的更高次幂都不是它们的公因子. 此外, 再没有其它整数整除 m 和 n, 因此 $2^2\cdot 3$ 就是 m 和 n 的最大公因子. 给出了 m 和 n 的素数幂分解式后, 我们可在必要处插入一些指数为零的素数, 使 m 和 n 被写成同样一些素数的乘积. 例如,

$$120=2^3\cdot 3^1\cdot 5^1\cdot 7^0,\quad 252=2^2\cdot 3^2\cdot 5^0\cdot 7^1.$$

一般地, 我们有

定理 3 若 $e_i\geqslant 0$, $f_i\geqslant 0$ $(i=1, 2, \cdots, k)$,

$$m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\quad n=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}, \tag{4}$$

则

$$(m, n)=p_1^{g_1}p_2^{g_2}\cdots p_k^{g_k},$$

其中 $g_i=\min(e_i, f_i)$, $i=1, 2, \cdots, k$.

我们将略去正式的证明，但要是你自己想证一下定理的正确性，当没有什么困难吧.

由因子分解唯一性定理可得，每一正整数均可写成这样的形式:

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}.$$

手头有了一张素数幂分解表，要求最大公因子就很容易了. 附录四表 C 就是素数幂分解表的一部分，它为一些大数给出了完整的素数幂分解式. 由于在另外几节中的某些习题要用此表，因此我们将它附在书后.

习　题

1. 求下列各数的素数幂分解式:
   (a) 111;　(b) 1234;　(c) 2345;
   (d) 3456;　(e) 4567;　(f) 111,111;
   (g) 999,999,999,999.
2. 证明下列命题不成立: 若 $d|ab$, 必有 $d|a$ 或 $d|b$.
3. 坦塔格利亚(Tartaglia, 1556 年)曾称: 下列和数

$$1+2+4,\ 1+2+4+8,\ 1+2+4+8+16,\ \cdots$$

   交替地为素数和合数，证明他错了.
4. (a) 迪布凡耳(DeBouvelles, 1509 年)曾称: 对所有 $n\geqslant 1$, $6n+1$ 和 $6n-1$ 中至少有一个是素数，证明他错了; 取 n= [illegible]
   (b) 说明有无限多个 n 使 $6n-1$ 和 $6n+1$ 同时为合数.
5. 相继的两个立方数之差总能被 2 整除吗?
6. 证明: 当且仅当 n 的素数幂分解式中每一指数都是偶数时，n 是一个平方数.
7. 相应于 k 次幂的命题应怎样说?
8. 一个素数能不能同时整除 n 和 $n+1(n\geqslant 1)$?
9. 证明: 当 $n>0$ 时, $n(n+1)$ 决不会是一个平方数.
10. (a) 验证 $2^5\cdot 9^2=2592$;

事实上. k_1n+l_1 与 k_2n+l_2 有无限多个 n 使其同时为合数 这只要取 $n=(k_1+l_1)(k_2+l_2)m+1$ 即可.

(b) 是否能有其它 a, b, 满足 $2^5 \cdot a^b = \overline{25ab}$?（这里, $25ab$ 表示 $2^5 \cdot a^b$ 的各位数字, 不是相乘.）

11. p 是什么素数时, $17p+1$ 是一个平方数?

12. (a) 求最小的整数 n 使 $n+1$, $n+2$ 和 $n+3$ 均为合数;

(b) 若 $n=5!+1$, 证明 $n+1, n+2, n+3$ 和 $n+4$ 都是合数;（关于记号"!", 见附录二.）

(c) 求由 1,000 个相继合数构成的序列.

13. 证明: 若 n 是合数, 2^n-1 也是合数.

14. 上述命题之逆成立吗?

15. 设 p 是合数 n 的最小素因子, 证明: 若 $p>n^{1/3}$, 则 n/p 是素数.

16. 下列命题是否正确: "若 p 和 q 整除 n, 且均大于 $n^{1/4}$, 则 n/pq 是素数"?

17. 定义 a 和 b 的**最小公倍数**（记为 $[a, b]$）为满足 $a|m$ 和 $b|m$ 的最小正整数 m.

(a) 求 $[12, 30]$ 和 $[pq, 2p^2]$, 其中 p 和 q 为不同的奇素数;

(b) 证明: 若 $a=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, $b=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$, 则 $[a, b]=p_1^{g_1}p_2^{g_2}\cdots p_k^{g_k}$, 其中 $g_i=\max(e_i, f_i)$ $(e_i\geqslant 0, f_i\geqslant 0)$, $i=1, 2, \cdots, k$;

(c) 由(b)和定理 3 推出: $[a, b]=ab/(a, b)$.

18. 在以下关于无限多素数的存在性证明中补上漏写部分: 设 $2, 3, \cdots, p_n$ 都是素数. 设 $N=2\cdot 3\cdots p_n$, 并假定 $N=ab$, 那么 $a+b>p_n$, 且 $p_i \nmid a+b$, $i=1, 2, \cdots, n$. 因此, $a+b$ 有一个大于 p_n 的素因子.

19. (a) 若 N 为奇数, 证明存在一个平方数, 当它加上 N 时仍为一个平方数;

(b) 若 $N+a^2=b^2$, N 具有怎样的因子?

(c) 对 1189 依次加上 $1^2, 2^2, 3^2, \cdots$, 直到认出一个平方数为止, 并借此对 1189 分解因子;（参见表 B.）

(d) 用同样方法对 9379 进行因子分解.

20. 确证下列素数判别法: 若 n 为大于 5 的奇数, 且存在互素整数 a 和 b, 使

$$a-b=n \quad 和 \quad a+b=p_1p_2\cdots p_k$$

（其中 $p_1, p_2, \cdots, p_k$ 是小于 $n^{1/2}$ 的奇素数）, 则 n 是素数.

21. 证明：小于 n^2 的所有奇素数恰是不包含在下列算术级数中的所有奇数：

$$r^2,\ r^2+2r,\ r^2+4r,\ \cdots,\ (\text{直到 } n^2),$$

而 $r=3, 5, 7, \cdots$，(直到 $n-1$)。

22. 设 $P_n=p_1p_2\cdots p_n$，且 $a_k=1+kP_n$，$k=0, 1, \cdots, n-1$，其中，$p_1, p_2, \cdots, p_n$ 是由小到大排列起来的素数：$2, 3, 5, 7, \cdots$。证明：当 $i\neq j$ 时，$(a_i, a_j)=1$。

§3 线性不定方程

考虑从一个古老问题变来的下述问题：

一只箱中装有多只蜜蜂和多只蜘蛛，它们共有 46 只脚，其中多少只脚是蜜蜂的？

如令 x 为箱中蜜蜂数，y 为蜘蛛数，则我们知

$$6x+8y=46. \tag{1}$$

这一方程有无限多组解，例如：

x	-1	0	6	$4\sqrt{2}$
y	$52/8$	$46/8$	$10/8$	$46/8-3\sqrt{2}$

但是，这些解都不满足问题的要求，因为我们要求 x 和 y 是整数，而且还应是正整数.

对这种方程求解时，解要限制在某类数中，它可以是正整数、负整数、有理数或任何其它类别的数．这种方程称为*丢番图方程*．亚历山大里亚城的丢番图(Diophantus，可能生活在公元 150 年左右)第一个提出并求解需求整数解和有理数解的问题．在本书后面某几节中，我们还要考虑其它丢番图方程，例如，

$$x^2+y^2=z^2,\quad x^2-2y^2=1,\quad x^4+y^4=z^4,$$

对它们要寻求整数解．这三个方程在实数和复数范围内都有无限多组解；但在整数范围内，第三个方程只有平凡解，即 x 和 y 中至少有一是零．而另一方面，第一个方程和第二个方程却都有无限多组整数解.

本节中，我们要考虑下列最简单的丢番图方程：线性不定

方程

$$ax+by=c,$$

其中 a, b, c 都是整数. 这里,我们还假定 a 和 b 都不为零; a 或 b 有一为零的情况到后面我们也要稍提一下. 我们想要找出 x 和 y 为整数的解. 方程 $ax+by=c$ 显然在有理数范围内具有无限多组解,从而在实数范围内也有无限多组解,写出来就是

$$x=t, \ y=(c-at)/b,$$

其中 t 为任意有理数. 但是,这样一个方程有可能根本没有整数解. 例如, $2x+4y=5$ 就没有整数解.

【练习 1】 为什么?

借助于§1 定理 4 和定理 5,我们可求 $ax+by=c$ 的全部整数解. 在此以前,让我们先用尝试法解决蜜蜂和蜘蛛问题(1). 用 2 除(1)的两端,我们有 $3x+4y=23$, 或

$$x=\frac{23-4y}{3}.$$

由于 x 和 y 必须是正整数,我们可令 $y=1, 2, 3, 4, 5$, 并计算相应的 x 值(若 $y>5$, 则 x 为负数):

y	1	2	3	4	5
x	19/3	5	11/3	7/3	1

因此,该不定方程有两组整数解: $x=5, y=2$ 和 $x=1, y=5$. 但原问题说明箱中有多只蜜蜂,故我们只要一个解答: 30 只脚属于蜜蜂. 尝试法有时是解不定方程的最好方法,但我们想要找出更有把握的办法来.

注意,如果我们能找出不定方程的一组解,那么我们就能找出它的无限多组解. (根据我们的约定,小写字母若未另加说明总代表整数, 说到"解"则总是指"整数解".)我们用引理 1 来证明这一点.

引理 1 如 x_0 和 y_0 为 $ax+by=c$ 的一组解，则对任何整数 t, x_0+bt, y_0-at 也是 $ax+by=c$ 的解.

证明 已知 $ax_0+by_0=c$. 因此,

$$a(x_0+bt)+b(y_0-at)=ax_0+abt+by_0-bat$$
$$=ax_0+by_0=c,$$

故 x_0+bt, y_0-at 也满足此方程. 例如，由观察我们知，$x=1$, $y=2$ 满足

$$5x+6y=17.$$

由引理 1 得，$x=1+6t$, $y=2-5t$(t 为任意整数)也是方程的解. 这样，我们可随意写出许许多多解来:

t	0	1	−1	3	−5	17	−1000
x	1	7	−5	19	−29	103	−5999
y	2	−3	7	−13	27	−83	5002

各对 x 与 y 都满足 $5x+6y=17$.

【练习 2】 用观察法求出 $x+5y=10$ 的一组解，并用它写出另外五组解来.

在有了下列引理之后，我们会看到，不失一般性，总可假定 $(a,\ b)=1$.

引理 2 若 $(a,\ b)\nmid c$, 则 $ax+by=c$ 无解; 而若 $(a,\ b)\mid c$, 则 $ax+by=c$ 有解.

证明 假定存在 x_0 和 y_0 使 $ax_0+by_0=c$. 因 $(a,\ b)\mid ax_0$, $(a,\ b)\mid by_0$, 所以，$(a,\ b)\mid c$. 反之，假定 $(a,\ b)\mid c$, 则有某一 m, 使 $c=m(a,\ b)$. 由 §1 引理 4, 我们知存在 r 和 s, 使

$$ar+bs=(a,\ b).$$

因此，
$$a(rm)+b(sm)=m(a,\ b)=c.$$

从而 $x=rm$, $y=sm$ 是一组解.

【练习 3】 下列不定方程中，哪几个是不可能方程？（若一个不定方程无解，我们就称它为不可能方程.）

(a) $14x+34y=90$; (b) $14x+35y=91$;

(c) $14x+36y=93$.

记 $d=(a, b)$. 引理 2 说明，若 $ax+by=c$ 有解，则 $d|c$. 令 $a=da'$, $b=db'$, $c=dc'$. 如用 d 除 $ax+by=c$，我们得

$$a'x+b'y=c';$$

这一方程与 $ax+by=c$ 有相同的解集. 由 § 1 定理 1 我们知，$(a', b')=1$. 因此，如果一个线性不定方程有解，我们就可通过解一个系数互素的方程而把解求出. 例如，练习 3 中前两个方程就分别等价于

$$7x+17y=45,\quad 2x+5y=13,$$

且有 $(7, 17)=(2, 5)=1$.

方程 $2x+5y=13$ 有一组解为 $x=4$ 和 $y=1$，而由引理 1 我们知，$x=4+5t$, $y=1-2t$（t 为任意整数）都是它的解. 在下一引理中，我们将证明，它们就是此方程的所有解. 一般说来，求丢番图方程所有解的问题与求若干组解的问题是很不相同的. 例如，方程

$$x^3+y^3=z^3+w^3$$

具有下列形式的解：

$$x=1-(s-3t)(s^2+3t^2),$$
$$y=-1+(s+3t)(s^2+3t^2),$$
$$z=s+3t-(s^2+3t^2)^2,$$
$$w=-s+3t+(s^2+3t^2)^2,$$

其中 s 和 t 可以是任意整数. 如果你有耐心的话，可用乘法来进行验证. 然而，并不是该方程的所有整数解都能用上面

公式来表示.

引理 3 假定 $ab\neq 0$, $(a, b)=1$, 且 x_0, y_0 是 $ax+by=c$ 的一组解, 则 $ax+by=c$ 的所有解可写为

$$x=x_0+bt,\ y=y_0-at,$$

其中 t 是整数.

证明 由引理 2 我们看到, 因为 $(a, b)=1$, 而对任何 c, 有 $1|c$, 故所述方程确实有解. 那么, 设 r, s 是 $ax+by=c$ 的任意解. 我们要证, $r=x_0+bt$, $s=y_0-at$ 必对某一整数 t 成立. 由 $ax_0+by_0=c$ 得

$$c-c=(ax_0+by_0)-(ar+bs)$$

即

$$a(x_0-r)+b(y_0-s)=0. \tag{2}$$

由于 $a|a(x_0-r)$, $a|0$, 我们有 $a|b(y_0-s)$. 但我们已假定 a 与 b 是互素的, 由 §1 定理 5 得 $a|(y_0-s)$. 便存在一个整数 t, 使

$$at=y_0-s. \tag{3}$$

代入(2)便得

$$a(x_0-r)+bat=0.$$

因为 $a\neq 0$, 我们可将它约去, 得

$$x_0-r+bt=0. \tag{4}$$

而(3)和(4)表明

$$s=y_0-at,\quad r=x_0+bt,$$

因 r, s 是任意解, 故引理得证.

在引理 3 中, 我们假定了 $ab\neq 0$. 如 $ab=0$, 解 $ax+by=c$ 的问题就非常简单. 若 $a=0$, 则 x 可取任意整数值, 而 y 可取一个值或无解, 依照 $by=c$ 在整数中有解或无解而定. 当 $b=0$ 时, 情况类似.

我们可以将引理1到引理3的结果总结如下：

定理1 若$(a, b)\nmid c$，则线性不定方程$ax+by=c(ab\neq 0)$无解；若$(a, b)|c$，则对$a'x+b'y=c'$（其中$a'=a/(a, b)$，$b'=b/(a, b)$，$c'=c/(a, b)$）可找到一组解$x=r, y=s$，且$ax+by=c$的所有解可写为

$$x=r+b't,\ y=s-a't,$$

其中t是任意整数.

在§5中，我们将看到如何利用同余式求解线性不定方程.

掌握上述定理的内容可能比实际求解线性不定方程要难一些．举一个例子，让我们求出$2x+6y=18$的所有解．除以公因子后，我们得$x+3y=9$．由观察法知，$y=0$，$x=9$是一组解．因此所有解可写为

$$x=9+3t,\ y=-t, \tag{5}$$

其中t为整数.

【练习4】 求$2x+6y=20$的所有解.

【练习5】 在正整数范围内求$2x+6y=18$的所有解．（注意，由(5)，这就相当于求整数t，使$9+3t>0$，$-t>0$.）

习　题

1．求下列方程的所有整数解：

(a) $x+y=2$;　　(b) $2x+y=2$;

(c) $15x+16y=17$;　　(d) $15x+18y=17$.

2．求下列方程的正整数解：

(a) $x+y=2$;　　(b) $2x+y=2$;

(c) $6x+15y=51$;　　(d) $7x+15y=51$.

3．求下列方程的负整数解：

(a) $6x-15y=51$;　　(b) $6x+15y=51$.



4．求下列方程组的正整数解：

$$x+y+z=31,$$
$$x+2y+3z=41.$$

5．假定一群蜈蚣、蝎子和蚯蚓共有 296 只脚和 35 个头，其中有多少条蚯蚓？（已知每只蝎子有 8 只脚，假定每条蜈蚣有 100 只脚.）

6．某人用 9 角 9 分钱买了 12 只水果(苹果和桔子)，每个苹果比每个桔子贵 3 分钱，且买的苹果数多于桔子数，问他买的苹果和桔子各多少？

7．某人出售羊和牛，共得 2890 元，羊每头 180 元，牛每头 290 元，问他卖出多少头牛？

8．用 30 张票面值为五分、一角和二角五分的钞票兑换 5 元钱，有多少种不同的兑换方法？

9．参加数论学习的某班由二年级、三年级和四年级的部分学生组成．若每个二年级学生缴费 1.25 元，每个三年级学生缴费 0.90 元，每个四年级学生缴费 0.50 元．全班 26 名学生，一共缴费 25 元，问每个年级各有多少名学生？

10．A 说："我们三人共有 100 元."B 说："对，如果你的钱是现有的 6 倍，我的钱是现有的 1/3，我们三人仍有 100 元."C 说："真不公平，我连 30 元钱都不满."问每人各有多少钱？

11．当安娜的年龄达到玛丽现在的年龄的 3/2 倍时，玛丽的年龄将是现在安娜的年龄的 5 倍，现在两人都未到达可以参加选举的年龄，问安娜是几岁？

12．假定 a, b, c 无大于 1 的公因子，证明 $ax+by+cz=1$ 的解可表示为

$$x=rt+crm+nb/d,$$
$$y=st+csm-na/d,$$
$$z=u-dm,$$

其中 m 和 n 是任意整数，r 和 s 满足 $ar+bs=d=(a, b)$，t 和 u 满足 $dt+cu=1$.

13．利用上述结果求解 $7x+8y+9z=1$.

14．某人到银行去兑换一张 d 元和 c 分的支票，出纳员出错，给了他 c

元和 d 分．此人直到用去 23 分后才发觉其错误，此时他发现还有 $2d$ 元和 $2c$ 分．在上述假定下，那张支票原来是多少钱？

15．安娜带 30 个蛋、巴尔巴拉带 40 个蛋到市场上出售．每人以 5 分一个蛋的价格卖出一部分，余下的蛋后来降价出售(以分计价，价格仍是整数)，各人卖得的钱数目相同．她们每人至少卖得了多少钱？

§4 同　余　式

同余式不但相当有趣，而且应用广泛，以后就要经常用到．任何尚未真正掌握同余式的人，都不能自称熟悉数论．利用同余式易证，形为 $8n+7$ 的整数，都不能写为三个平方数之和，这是说明同余式用处的一例，后面我们将要证明这一点．

当且仅当 $m\mid(a-b)$时．我们称 a 与 b 对模 m 同余，用记号可写为 $a\equiv b\pmod m$（这里总设 $m>0$）．

例如，$1\equiv5\pmod 4$，$-2\equiv9\pmod{11}$，$6\equiv20\pmod 7$，$720\equiv0\pmod{10}$．

【练习 1】　下列各式正确吗？$91\equiv0\pmod 7$；$3+5+7\equiv5\pmod{10}$；$-2\equiv2\pmod 8$；$11^2\equiv1\pmod 3$．

本质上，$m\mid(a-b)$和 $a\equiv b\pmod m$只不过是同一性质的不同表示法而已．但是，一种好的记号可以显示出一些新的结果，而没有这种记号，要看出这些结果可能就会困难得多．同余式的记号是高斯(Gauss)在 1800 年左右首创的，它看起来有点象等式的记号．事实上，我们以后就会看到，同余式和等式有着许多共同的性质．此外，这一记号也暗示了与通常的代数运算相似的许多结果．

可用另一种方式看待同余式：

定理 1　当且仅当存在一整数 k 使 $a=b+km$ 时，

$$a\equiv b\pmod m.$$

证明　设 $a\equiv b\pmod m$．那么，由同余式定义，$m\mid(a-b)$．又根据整除定义知，存在一整数 k，使 $km=(a-b)$，故 $a=b+$

km. 反过来, 设 $a=b+km$, 也可证得 $a\equiv b \pmod m$.

【练习 2】 完成这一定理的证明.

定理 2 每一整数恰与 0, 1, …, $m-1$ 中一数同余 $(\bmod m)$.

证明 记 $a=qm+r$, 其中 $0\leqslant r<m$. 由 § 1 定理 2 知, q 和 r 是唯一确定的. 由于 $a\equiv r \pmod m$, 定理得证.

我们称上述定理中的数 r 为 a 的最小剩余 $(\bmod m)$. 例如, 71 对模 2, 3, 5, 7 和 11 的最小剩余分别为 1, 2, 1, 1 和 5.

【练习 3】 23, 29, 31, 37 和 41 的最小剩余 $(\bmod 11)$ 各为什么数?

看待同余式还有一种方式:

定理 3 当且仅当 a 和 b 用 m 相除留下相同余数时,

$$a\equiv b \pmod m.$$

证明 若 a 和 b 用 m 相除留下相同余数 r, 则

$$a=q_1m+r, \quad b=q_2m+r,$$

q_1 和 q_2 为某两个整数. 由此得

$$a-b=(q_1m+r)-(q_2m+r)=m(q_1-q_2).$$

根据整除定义, 我们有 $m\mid(a-b)$. 由同余式定义, 我们得出结论: $a\equiv b \pmod m$. 为了证明其逆, 设 $a\equiv b \pmod m$. 那么, $a\equiv b\equiv r \pmod m$, 其中 r 是对模 m 的一个最小剩余. 然后由定理 1,

$$a=q_1m+r, \quad b=q_2m+r,$$

q_1 和 q_2 为某两个整数; 因 $0\leqslant r<m$, 故定理得证.

由定理 1 和定理 3 可知, "$n\equiv 7 \pmod 8$", "$n=7+8k$, k 为某一整数"和"n 用 8 相除留下余数 7"这三句话是同一件事的三种不同说法.

【练习 4】 用另外三种方式说明"n 是奇数".

【练习 5】 证明：当且仅当 $a\equiv 0 \pmod p$ 时，$p|a$.

正如你在下面三个练习中将要证明的那样，同余式与等式具有许多相同的性质.

【练习 6】 证明：

(a) 对一切整数 a，$a\equiv a \pmod m$；

(b) 若 $a\equiv b \pmod m$，则 $b\equiv a \pmod m$；

(c) 若 $a\equiv b \pmod m$，$b\equiv c \pmod m$，则 $a\equiv c \pmod m$.

【练习 7】 证明：若 $a\equiv b \pmod m$，则

$$a+c\equiv b+c \pmod m,$$

其中 c 为任意整数.

【练习 8】 证明：若 $a\equiv b \pmod m$，则 $ac\equiv bc \pmod m$，其中 c 为任意整数.

练习 6, 7 和 8 说明，同余式可象等式那样进行代换. 例如，若 $x\equiv 2 \pmod 5$，则

$$2x^2-x+3\equiv 2\cdot 4-2+3\equiv 9\equiv 4 \pmod 5.$$

或许你想要详细证明这一点，只要记住反复应用练习 8, 7 和 6(c)就行了. 本例中成立的事在一般情况下也成立.

虽然，对所有整数 a, b 和 c，若 $ab=ac$，$a\neq 0$，就有 $b=c$，但若说，由 $ab\equiv ac \pmod m$，$a\not\equiv 0 \pmod m$，也有 $b\equiv c \pmod m$，这就不对了.（记号"$\not\equiv$"表示"不同余".）例如，

$$3\cdot 4\equiv 3\cdot 8 \pmod{12}, \quad 但 \quad 4\not\equiv 8 \pmod{12}.$$

【练习 9】 对模 10，举出一个相仿的例子.

尽管我们不能随便消去一个数，但由下列定理可知，也不是什么结论都不能得出.

定理 4 若 $ac\equiv bc \pmod m$，$(c, m)=1$，则 $a\equiv b \pmod m$.

证明 由同余式定义，$m|(ac-bc)$，即 $m|c(a-b)$. 因

$(m, c)=1$, 由§1定理5, 我们得 $m \mid (a-b)$, 即 $a \equiv b \pmod m$.

【练习10】 x 为何值时, 满足

(a) $2x \equiv 4 \pmod 7$?　　　　(b) $2x \equiv 1 \pmod 7$?

(提示: 对于(b), 利用 $1 \equiv 8 \pmod 7$.)

于是, 如果同余式两端有一公因子与模互素, 我们就可将它消去. 现在我们考虑公因子与模不互素的情况.

定理5 若 $ac \equiv bc \pmod m$, $(c, m)=d$, 则

$$a \equiv b \pmod{m/d}.$$

证明 若 $ac \equiv bc \pmod m$, 则 $m \mid c(a-b)$, 即 $m/d \mid (c/d) \times (a-b)$. 因我们知 $(m/d, c/d)=1$, 故由§1定理5, 我们得 $m/d \mid (a-b)$, 所以 $a \equiv b \pmod{m/d}$.

换句话说, 同余式两端的公因子总可消去, 只要我们将该因子与模的最大公因子去除模即可. 例如, 由

$$30x \equiv 27 \pmod{33},$$

可得

$$10x \equiv 9 \pmod{11}.$$

【练习11】 x 为何值时, 满足 $2x \equiv 4 \pmod 6$?

现在我们就可看到, 要证明形为 $8n+7$ 的任何整数都不会是三个平方数之和是何等容易啊! 假如 $k=8n+7$ 是三个平方数之和, 那么 $k \equiv 7 \pmod 8$, 且对某些整数 a, b 和 c, 有 $k=a^2+b^2+c^2$. 因此,

$$a^2+b^2+c^2 \equiv 7 \pmod 8.$$

现在我们证明, 对任何整数 a, b 和 c, 上述同余式都不能成立. 对模8, x^2 可取哪些值? 每一整数的最小剩余(mod 8)必为0, 1, 2, 3, 4, 5, 6, 7中一数. 而对模8, 还有

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 1,\ 4^2 \equiv 0,\ 5^2 \equiv 1,$$
$$6^2 \equiv 4,\ 7^2 \equiv 1.$$

于是, 任一整数的平方对模8必与0, 1和4三数中之一数同

余，而要从 0，1，4 中取三个数相加，使其和与 7 同余 $(\bmod 8)$ 是不可能的.（你能得到的最接近的结果是 $1+1+4\equiv 6$ 和 $0+4+4\equiv 8 (\bmod 8)$.）因此，对任何整数 a，b 和 c，$a^2+b^2+c^2$ 决不会与 7 同余 $(\bmod 8)$. 故 $a^2+b^2+c^2=8n+7$ 是一个不可能成立的式子.

作为同余式的另一应用，我们要说明为什么可用“弃九法”检查出加法和乘法中的错误. 可能你在算术中从未学过“弃九法”，这里介绍一下：给定某一加法，比方说

$$3141+5926+5358=14325,$$

将各加数的各位数字相加，就有

$$3+1+4+1=9,$$

$$5+9+2+6=22,$$

$$5+3+5+8=21.$$

如果这些和数中，有些数仍是多位数，那么再做一次这样的加法：

$$2+2=4, \quad 2+1=3.$$

最后总可得到一位数. 将它们相加，

$$9+4+3=16,$$

再用此法：$1+6=7$，最后我们求得一个一位数，作为这些加数的“检验数”. 用同样的方法我们可得和数的检验数：

$$1+4+3+2+5=15, \quad 1+5=6.$$

如果原加法做得对，这两个检验数本应该相同. 而在此例中，检验数不一样，故加法做错了. 注意，弃九法并不能确保某一计算是正确的. 例如，对

$$10+11=30$$

施行弃九法时，就查不出错来，因为两个检验数都是 3. 不过，有些普通的错误，如忘了进位等，弃九法还是可以检查出来

的．这一方法也适用于乘法．容易看出，下列乘法的结果错了：

$$314\cdot159=49826,$$

因为左端的检验数为3（314的检验数为8，159的检验数为6；相乘后，我们知积的检验数为$8\cdot6=48$，或3），而右端的检验数为2，因为$4+9+8+2+6=29$．如果乘法做得对，这两个检验数本来应是一样的．

【练习12】 用弃九法验算：

(a) $123+456+789=1268$;

(b) $271\cdot828=224288$.

现在我们来证为什么上述方法的确可行．其根据是：

引理1 $10^n\equiv1\pmod 9$，对$n=1, 2, \cdots$都成立．

证明 $10^n-1=999\cdots999$（共有n个9），它显然能被9整除．

由引理1，可得

定理6 每一整数与它的各位数字之和对模9同余．

证明 取一整数n，设其各位数字可写为

$$d_kd_{k-1}d_{k-2}\cdots d_1d_0,$$

即 $$n=d_k10^k+d_{k-1}10^{k-1}+d_{k-2}10^{k-2}+\cdots+d_110^1+d_010^0.$$

由引理1，我们知

$$n\equiv d_k+d_{k-1}+d_{k-2}+\cdots+d_0\pmod 9,$$

这正是我们所要证明的．

例如，$3141=3+1+4+1\equiv9\equiv0\pmod 9$，我们便知3141可被9整除．

由此易知，算术运算中进行“弃九”，就相当于对模9考虑同余．例如，

$$3141+5926+5358=14325,$$

定理 6 说明，左端与下列数同余：

$$3+1+4+1+5+9+2+6+5+3+5+8\equiv 52$$
$$\equiv 7 \pmod 9,$$

而右端与 6 同余 $(\bmod 9)$. 如果两个数不同余 $(\bmod 9)$, 就不会相等. 因而 14325 不是正确的和数.

习　题

1. 证明：若 $a\equiv b \pmod m$，则 $a^2\equiv b^2 \pmod m$.
2. 证明下列命题不成立：若 $a^2\equiv b^2 \pmod m$，则 $a\equiv b \pmod m$.
3. 下列命题是否成立：由 $a\equiv b \pmod m$，可得 $a^2\equiv b^2 \pmod{m^2}$？
4. 若 $k\equiv 1 \pmod 4$，则 $6k+5$ 与什么数同余 $(\bmod 4)$？
5. 证明：每个素数(2 除外)与 1 或 3 同余 $(\bmod 4)$.
6. 证明：每个素数(2 和 3 除外)与 1 或 5 同余 $(\bmod 6)$.
7. 素数(2, 3 和 5 除外)可与哪些数同余 $(\bmod 30)$？
8. 在乘法 $3145\cdot 92653=2910__93995$，积中有一位数字遗漏，而其它数字是正确的，遗漏之数字是什么？
9. 证明：若 n 的末位数为 d，则 $n^2\equiv d^2 \pmod{10}$.
10. 证明：任何平方数的末位数不能是 2, 3, 7 或 8.
11. 证明：任何三角形数的末位数不会是 2, 4, 7 或 9. (一个三角形数可写成 $n(n+1)/2$ 的形式.)
12. 证明：若 $d|m$，$a\equiv b \pmod m$，则 $a\equiv b \pmod d$.
13. 证明：相继的两个立方数之差决不能被 3 整除.
14. 证明：相继的两个立方数之差决不能被 5 整除.
15. 证明：若一个整数的各位数字之和被 3 整除，则此数也被 3 整除.
16. (a) 证明：$10^k\equiv(-1)^k \pmod{11}$，$k=0, 1, 2, \cdots$；
    (b) 推证：$d_k10^k+d_{k-1}10^{k-1}+\cdots+d_1 10+d_0\equiv d_0-d_1+d_2-d_3+\cdots+(-1)^k d_k \pmod{11}$；
    (c) 推出被 11 整除的判别方法.
17. 甲说："27,182,818,284,590,452 可被 11 整除."乙说："不对."谁是正确的？

18．证明：若 p 为素数，且 p 不能整除 $a_1, a_2, \cdots, a_{p-1}$ 中任何一数或任何两数之差，则 $a_1, a_2, \cdots, a_{p-1}$ 按某一次序分别与 1, 2, …, $p-1$ 同余 $(\bmod p)$．

19．1968 年二月份有五个星期四．在 2100 年以前，还会有哪几年有这种二月份？

20．一个数，如果倒过去读仍为此数，称为**回文数**，如 22，1331，935686539 等．

(a) 证明：每个四位数回文数被 11 整除；

(b) 每个六位数回文数都能被 11 整除吗？

21．证明：对所有 a，$a^5 \equiv a \pmod{10}$．

22．求一个整数 n，使 $n\equiv 1 \pmod 2$，$n\equiv 0 \pmod 3$，$n \equiv 0 \pmod 5$ 同时成立．你能找到无限多个这样的数吗？

23．证明：若 $n\equiv 4 \pmod 9$，则 n 不能写为三个数的立方和．

24．证明：若 $x\equiv 1 \pmod{m^k}$，其中 $k>0$，$m\geqslant 1$，则 $x^m\equiv 1 \pmod{m^{k+1}}$．

25．若 $n=31,415,926,535,897$，再令

$$f(n)=897-535+926-415+031=904.$$

导出 f 的定义，且证明：若 $7|f(n)$，则 $7|n$；若 $11|f(n)$，则 $11|n$；若 $13|f(n)$，则 $13|n$．检验 118,050,660 能否为 2，3，5，7，11 和 13 整除．

§5 线性同余式

定义了同余式并研究了它们的某些性质以后，很自然地要看一看涉及到未知数的同余式，如 $3x\equiv4 \pmod 5$，$x^{17}+3x-3\equiv0 \pmod{31}$，等等. 而且，我们还要知道，如果这种同余式可以求解，具体应如何进行. 这种同余式中，最简单的是线性同余式：$ax\equiv b \pmod m$，它就是本节研究的对象. 当且仅当有整数 x 和 k 满足 $ax=b+km$ 时，同余式 $ax\equiv b \pmod m$ 有解. 因此，解线性同余式的问题本质上与解线性不定方程问题是相同的，而本节定理 1 说到底也是与 §3 定理 1 相同的，我们只是用不同的记法来表示相同的概念而已. 不过，这两种记法很不相同，进行重复的叙述，不但不会令人厌倦，反倒可能发人深思.

我们注意到，要是存在一个整数满足 $ax\equiv b \pmod m$，就必存在无限多个这样的整数. 这是因为，如若 $ar\equiv b \pmod m$，则对任意整数 k，有 $a(r+km)\equiv ar\equiv b \pmod m$，因而 $r+m$，$r+2m$，$\cdots$，$r-m$，$r-2m$，$\cdots$ 这些整数都满足上述同余式. 在 $r+km(k=0, \pm1, \pm2, \cdots)$ 这些整数中，恰有一个(比方说 s)满足 $0\leqslant s<m$，这是因为，每个整数都介于 m 的相继两个倍数之间. 若 r 对某个 k 满足 $km<r<(k+1)m$，则有 $0\leqslant r-km<m$，我们就可令 $s=r-km$. 我们将这样一个数挑出，并称它为 $ax\equiv b \pmod m$ 的一个解. 故解就是这样一个数 r，它满足 $ar\equiv b \pmod m$，且为一个最小剩余 $\pmod m$. 例如，$x=2, 9, 16, \cdots, -5, -12, -19, \cdots$ 均满足同余式 $2x\equiv$

4(mod 7)，它们都包含在命题 $x\equiv 2 \pmod 7$ 中，也都包含在命题 $x\equiv 9 \pmod 7$ 中，但我们约定，只把 2 称为解，因为它是对模 7 的最小剩余.

与我们熟悉的线性方程 $ax=b$ 不同，线性同余式

$$ax\equiv b \pmod m$$

可以无解、只有一解或有许多解. 例如，$x=2$ 满足

$$2x\equiv 1 \pmod 3,$$

但作为最小剩余(mod 3)无其它 x 的值能满足此式，因而此式只有一解，即为 2. 同余式 $2x\equiv 1 \pmod 4$ 无解，因为对任何 x 都不可能有 $4\mid(2x-1)$. ($2x-1$ 是奇数，它不是 4 的倍数.) 同余式 $2x\equiv 4 \pmod 6$ 就有两解: 2 和 5.

【练习 1】 对模 12 构造几个同余式，使之分别为无解、有一解和有多个解.

【练习 2】 下列同余式中，哪些无解?

(a) $3x\equiv 1 \pmod{10}$; (b) $4x\equiv 1 \pmod{10}$

(c) $5x\equiv 1 \pmod{10}$; (d) $6x\equiv 1 \pmod{10}$,

(e) $7x\equiv 1 \pmod{10}$.

【练习 3】(选做) 做了练习 2 后，你是否能猜出一条规则，以判别何时同余式无解?

我们现在就来着手证明一个定理，它使我们在考察一个线性同余式时能够看出它有多少个解.

引理 1 若 $(a, m)\nmid b$，则 $ax\equiv b \pmod m$ 无解.

证明 我们将证明在逻辑上与此等同的一件事: 若 $ax\equiv b \pmod m$ 有解，则 $(a, m)\mid b$. 假定 r 是一解，则 $ar\equiv b \pmod m$. 由同余式定义，$m\mid(ar-b)$，或由“整除”定义，对某一 k 有 $ar-b=km$. 因 $(a, m)\mid a$, $(a, m)\mid km$，故得 $(a, m)\mid b$.

例如，$6x\equiv 7 \pmod 8$ 就没有解.

引理 2 若 $(a, m)=1$，则 $ax\equiv b \pmod m$ 恰有一解.

证明 因 $(a, m)=1$，我们知，存在整数 r 和 s，使

$$ar+ms=1.$$

乘上 b 即得

$$a(rb)+m(sb)=b.$$

由此可得 $arb-b$ 是 m 的一个倍数，或

$$a(rb)\equiv b \pmod m.$$

rb 对模 m 的最小剩余即为其线性同余式之一解.

余下要证明的是此同余式不能多于一解. 假定 r 和 s 均为解，换言之，

$$ar\equiv b \pmod m,\quad as\equiv b \pmod m,$$

可知 $ar\equiv as \pmod m$. 由于 $(a, m)=1$，我们可用上节定理 4 消去公因子，得 $r\equiv s \pmod m$，也即 $m\mid(r-s)$. 但 r 和 s 均为最小剩余 $(\bmod m)$，故

$$0\leqslant r<m,\quad 0\leqslant s<m.$$

因此，$-m<r-s<m$. 连同 $m\mid(r-s)$，就可得 $r-s=0$，或 $r=s$，即解是唯一的. 上述论据具有相当大的普遍性，常用得到：若两个对模 m 的最小剩余对模 m 同余，那么它们必相等.

观察法是求解模较小的同余式的一种方法，另一种方法是代入变量的所有可能值. 但最好的方法是变换其系数，使之有可能进行消去的步骤. 例如，解 $4x\equiv 1 \pmod{15}$，我们将它写为

$$4x\equiv 1\equiv 16 \pmod{15},$$

消去 4 得 $x\equiv 4 \pmod{15}$. 再举一例，让我们求解

$$14x\equiv 27 \pmod{31}.$$

由

$$14x\equiv 27\equiv 58 \pmod{31},$$

我们得 $7x\equiv 29 \pmod{31}$. 继续逐次加上 31，使之能够消去 7：

$$7x\equiv 29\equiv 60\equiv 91 \pmod{31},$$

故我们得 $x\equiv 13 \pmod{31}$，13 即为其解.

在解线性不定方程时，这也是可使用的最好方法. 方程 $ax+by=c$ 就是两个同余式:

$$ax\equiv c \pmod b,\qquad by\equiv c \pmod a.$$

我们可选其中任一个并解出其变量，然后将结果代入原方程而求得其全部解. 例如，我们来解 $9x+16y=35$，由此得

$$16y\equiv 35 \pmod 9.$$

改变系数，得

$$7y\equiv 35 \pmod 9.$$

由此可得 $y\equiv 5 \pmod 9$，也即对某一整数 t，有 $y=5+9t$，将此代入原方程，得

$$9x+16(5+9t)=35,$$

或 $9x+144t=-45$，即 $x+16t=-5$. 因而我们求得了所有解:

$$x=-5-16t,\ y=5+9t,$$

t 是整数.

【练习 4】 解下列同余式和不定方程:

(a) $8x\equiv 1 \pmod{15}$;　　　(b) $9x+10y=11$.

我们现在考虑 a 和 m 不一定互素的情况.

引理 3 若 $(a, m)\mid b$，则 $ax\equiv b \pmod m$ 恰有 (a, m) 个解.

证明 我们将作出同余式的 (a, m) 个解，然后证明没有其它解. 令 $d=(a, m)$，并设

$$a=da',\ b=db',\ m=dm'.$$

由 § 4 定理 5，我们有

(1)　　$a'x\equiv b' \pmod{m'}$，　且　$(a', m')=1$,

后式由 § 1 定理 1 得出. 将引理 2 用于(1)中同余式，得知它

恰有一解，称为解 r. 我们断言，下列 d 个数

(2) $$r,\ r+m',\ r+2m',\ \cdots,\ r+(d-1)m'$$

均为 $ax\equiv b\pmod m$的解. 首先，这些数之每一个都满足此同余式，因为对 $k=1,\ 2,\ \cdots,\ d-1$, 我们有

$$a(r+km')=da'r+da'km'=a'rd+a'k(m'd).$$

由于 $a'r\equiv b'\pmod{m'}$, $m'd=m$, 故有

$$a'rd+a'k(m'd)\equiv b'd+a'km\equiv b'd\equiv b\pmod m.$$

即 $$a(r+km')\equiv b\pmod m.$$

其次，(2)中各数都是最小剩余$\pmod m$，因为对 $k=0,\ 1,\ \cdots,\ d-1$，有

$$0\leqslant r+km'\leqslant r+(d-1)m'<m'+(d-1)m'$$
$$=dm'=m.$$

第三，(2)中任意两数互不同余$\pmod m$，因为它们是不同的最小剩余$\pmod m$. 这样，我们就证明了 $ax\equiv b\pmod m$ 有$(a,\ m)$个解.

剩下来要证明它没有其它的解. 设 r 是(2)中的解，而 s 为 $ax\equiv b\pmod m$的任一解，我们要证 s 是(2)中的一个数. 我们有

$$ar\equiv as\equiv b\pmod m.$$

由§4 定理 5 可得 $r\equiv s\pmod{m'}$，即 $s-r=km'$，或对某 k，有

$$s=r+km'.$$

但 s 是一个最小剩余$\pmod m$，而形为 $r+km'$ 的所有最小剩余$\pmod m$都出现在(2)中，因此 s 是(2)中的一个数. 因为 s 是任一解，故知(2)中的解就是所有解，引理得证.

让我们来看一个例子. 考虑 $6x\equiv 15\pmod{33}$；引理 3 说明，该同余式恰有三个解. 消去一个 3，我们得 $2x\equiv 5\pmod{11}$，用通常的方法求解，

$$2x\equiv 5\equiv 16 \pmod{11},\quad x\equiv 8 \pmod{11}.$$

即 $6x\equiv 15 \pmod{33}$ 可为任何 $x\equiv 8 \pmod{11}$ 所满足，而后式包括的最小剩余 $(\bmod\ 33)$ 有 8, 19, 30, 它们就是原同余式的三个解.

【练习 5】 确定下列各同余式的解的个数:

$3x\equiv 6 \pmod{15}$, $4x\equiv 8 \pmod{15}$,

$5x\equiv 10 \pmod{15}$, $6x\equiv 11 \pmod{15}$,

$7x\equiv 14 \pmod{15}$.

【练习 6】 求出 $5x\equiv 10 \pmod{15}$ 的所有解.

我们可将引理 1 到引理 3 的几个结果总结于下列定理中:

定理 1 若 $(a, m)\nmid b$, 则 $ax\equiv b \pmod{m}$ 无解; 若 $(a, m)\mid b$, 则它恰有 (a, m) 个解.

【练习 7】 解出练习 5 中其它各个同余式.

这就完成了对单个线性同余式的分析. 在本节以下部分中，我们要考虑一种特殊的线性同余式组，并要证明理论上非常重要的"中国剩余定理". 这个定理的取名是由于某些古代中国的文稿载有类似于如下的一些问题[注]: "求一个数，它用 3 除余 2，用 5 除余 4，用 7 除余 6." 用我们的记号，这个问题就是求 x，满足

$$x\equiv 2 \pmod{3},\quad x\equiv 4 \pmod{5},\quad x\equiv 6 \pmod{7}.$$

【练习 8】 验证: 104 满足上面三个同余式.

【练习 9】(选做) 求出无限多个其它的数，它们满足这三个同余式.

定理 2(中国剩余定理) 设 $i\neq j$ 时, $(m_i, m_j)=1$, 则同

[注] 在《孙子算经》中，不但提出了这种问题，而且还给出了解答. ——译校者注

余式组

(3) $$x\equiv a_i(\bmod m_i),\quad i=1,\ 2,\ \cdots,\ k,$$

对模 $m_1m_2\cdots m_k$ 有唯一解.

在证明此定理以前,我们先考虑一个例子,它包含了证明的思想,并能说明如何实际求出这个唯一的解. 让我们寻找 x,它满足

$$x\equiv 1(\bmod 3),x\equiv 2(\bmod 5),\ x\equiv 3(\bmod 7).$$

第一个同余式得出,对某 k_1, 有 $x=1+3k_1$. 将此代入第二个同余式,则 k_1 必须满足

$$1+3k_1\equiv 2(\bmod 5);$$

因此 $k_1\equiv 2(\bmod 5)$. 也即对某 k_2, 有 $k_1=2+5k_2$, 因而

$$x=1+3k_1=1+3(2+5k_2)=7+15k_2,$$

它满足前面两个同余式. 若 x 还满足第三个同余式, 我们必有

$$7+15k_2\equiv 3(\bmod 7),$$

这就意味着 $k_2\equiv 3(\bmod 7)$. 因此,

$$x=7+15(3+7k_3)=52+105k_3,$$

对于任何 k_3,上式都满足所有三个同余式. 换一种方法来说,所有 $x\equiv 52(\bmod 105)$都满足这三个同余式. 事实上, 52 即为对模 105 的那个唯一解.

定理 2 的证明 我们首先用归纳法证明, (3)有一解. 当 $k=1$ 时, 这个结果是明显的. 让我们考虑 $k=2$ 的情况. 若 $x\equiv a_1(\bmod m_1)$, 则对某 k_1, 有 $x=a_1+k_1m_1$. 若还有

$$x\equiv a_2(\bmod m_2),$$

则 $$a_1+k_1m_1\equiv a_2(\bmod m_2),$$

或 $$k_1m_1\equiv a_2-a_1(\bmod m_2).$$

由于$(m_1,\ m_2)=1$, 我们知, 这个同余式对于未知数 k_1 有对模

m_2 的唯一解，把它称为 t．则对某 k_2，有 $k_1=t+k_2m_2$，且

$$x=a_1+(t+k_2m_2)m_1\equiv a_1+tm_1 \pmod{m_1m_2}$$

满足这两个同余式．

假设当 $k=r-1$ 时，同余式组(3)有一解$\pmod{m_1m_2\cdots m_k}$，即同余式组

$$x\equiv a_i \pmod{m_i},\quad i=1,\ 2,\ \cdots,\ r-1,$$

有一解 s．而同余式组

$$x\equiv s \pmod{m_1m_2\cdots m_{r-1}},\ x\equiv a_r \pmod{m_r}$$

也应有一解$\pmod{m_1m_2\cdots m_{r-1}m_r}$，这和 $k=2$ 时的情况正好一样，因为$(m_1m_2\cdots m_{r-1},\ m_r)=1$(这一论断之所以正确是因为整除任一 $m_i(i=1,\ 2,\ \cdots,\ r-1)$ 的素数都不能整除 m_r)．

我们还易见其解是唯一的．若 r 和 s 是同余式组的两个解，则

$$r\equiv s\equiv a_i \pmod{m_i},\quad i=1,\ 2,\ \cdots,\ k,$$

故 $m_i|(r-s)$，$i=1,\ 2,\ \cdots,\ k$．这样，$r-s$ 就是 $m_1,\ m_2,\ \cdots,\ m_k$ 的一个公倍数．由于这些模两两互素，我们就有 $m_1m_2\cdots m_k|(r-s)$．但因 r 和 s 是对模 $m_1m_2\cdots m_k$ 的最小剩余，

$$-m_1m_2\cdots m_k<r-s<m_1m_2\cdots m_k,$$

因而，$r-s=0$．

习　　题

1．求解下列同余式：

(a) $2x\equiv 1 \pmod{17}$；　　(b) $3x\equiv 1 \pmod{17}$；

(c) $3x\equiv 6 \pmod{18}$；　　(d) $4x\equiv 6 \pmod{18}$；

(e) $40x\equiv 191 \pmod{6191}$．

2．对模 20 作线性同余式，使其无解、有唯一解或有多个解．你能作出有 20 个解的同余式吗？

3．一个线性同余式(mod 20)的解数有哪几种可能情况？

4. 求解下列同余式组:

(a) $x\equiv1(\bmod 2)$, $x\equiv1(\bmod 3)$;

(b) $x\equiv1(\bmod 2)$, $x\equiv1(\bmod 3)$, $x\equiv6(\bmod 7)$;

(c) $x\equiv3(\bmod 5)$, $x\equiv5(\bmod 7)$, $x\equiv7(\bmod 11)$;

(d) $2x\equiv1(\bmod 5)$, $3x\equiv2(\bmod 7)$, $4x\equiv1(\bmod 11)$;

(e) $x\equiv31(\bmod 41)$, $x\equiv59(\bmod 26)$

5. 求解 $9x\equiv4(\bmod 2401)$.

6. 数学系某次游行中,参加者 4 人一排, 余下 1 人; 5 人一排,余下 2 人;7 人一排,余下 3 人. 问该系有多少人参加了游行?

7. 求最小的奇数 n, $n>3$, 使 $3|n$, $5|(n+2)$, $7|(n+4)$.

8. 求一非零的最小整数,使其一半是一个平方数, 其 1/3 是一个立方数,其 1/5 是一个五次方数.

9. 求 7 的一个倍数,使其分别被 2, 3, 4, 5, 6 相除时,余数都是 1.

10. 48, 49, 50 这三个相继整数中,每个数都有一个平方因子.

(a) 求 n,使 $3^2|n$, $4^2|(n+1)$, $5^2|(n+2)$;

(b) 你能否找到一个 n,使 $2^2|n$, $3^2|(n+1)$, $4^2|(n+2)$?

11. 若 $x\equiv r(\bmod m)$,且 $x\equiv s(\bmod m+1)$,证明:

$$x\equiv r(m+1)-sm(\bmod m(m+1)).$$

12. 求解 x 和 y:

(a) $x+2y\equiv3(\bmod 7)$, $3x+y\equiv2(\bmod 7)$;

(b) $x+2y\equiv3(\bmod 6)$, $3x+y\equiv2(\bmod 6)$.

13. 哪三个正整数与 3, 5, 7 分别相乘所得之积再被 20 相除所得之余数是公差为 1 的算术级数且相应的商分别依次等于这些余数?

14. 考虑同余式组:

$$x\equiv a_i(\bmod m_i),\quad i=1, 2, \cdots, k,$$

其中各模两两互素. 设

$$M_i=m_1m_2\cdots m_k/m_i,\quad i=1, 2, \cdots, k,$$

用 S_i 表示 $M_ix\equiv1(\bmod m_i)$的解, $i=1, 2, \cdots, k$. 证明:

$$S=a_1S_1M_1+a_2S_2M_2+\cdots+a_kS_kM_k$$

满足同余式组中各式,并使用上述方法解 4(b)中的同余式组.

15. 求最小整数 n, $n>2$, 使 $2|n$, $3|(n+1)$, $4|(n+2)$, $5|(n+3)$, $6|(n+4)$.

16. 假定同余式组

$$x\equiv a_i(\bmod m_i),\quad i=1,\ 2,\ \cdots,\ k$$

中各模不是两两互素，求该同余式组有解时 a_i 必须满足的条件.

17. 在数列 a, $2a$, $3a$, $\cdots$, ba 中，有多少个数是 b 的倍数?

§6 费马定理和威尔逊定理

本节中，我们将证明

定理 1(费马定理) 若 p 为素数，$(a, p)=1$，则

$$a^{p-1}\equiv 1(\bmod p).$$

这一定理由费马(Fermat)在 1640 年提出，但未加证明，它对数论的发展极为重要. 我们将看到，它是研究二次同余式的关键，并且还有许多其它的应用. 它的叙述和证明很简单，作用却很大. 我们还要证明

定理 2(威尔逊定理) p 为素数的充要条件为

$$(p-1)!\equiv -1(\bmod p).$$

(关于阶乘记号"!"，可参见附录二.)

证明这一定理所用的方法与费马定理的证明方法相近，它对二次同余式的研究也有帮助. (威尔逊定理实际上不属于威尔逊(Wilson)，他曾猜想这个定理是正确的，并就此事写信给华林(Waring)，后者在 1770 年未加证明就将它发表. 威尔逊并不是第一个作出这一猜想的人，莱布尼茨(Leibniz)在 1682 年就已发现了它，但第一个证明却是由拉格朗日(Lagrange)在华林宣布这一定理后不久给出的.)威尔逊定理之所以重要，原因在于，它给出了一个数是素数的一个充要条件. 因此，就理论上说来，决定一给定数是否为素数的问题已经完全解决. 但对于大整数，计算起来困难很大. 对于一个不太大的素数

$p=162,259,276,829,213,363,391,578,010,288,127,$

计算$(p-1)!$的最小剩余$(\bmod p)$大约需要做10^{33}次两个33位数的乘法，接着还要用p相除，即便使用我们最快的计算机也嫌太慢了．举例来说，人们可把两件事作一比较，一件是计算$12!(\bmod 13)$，另一件是验证13不能被2和3整除，看一看所费的功夫各是多少．

证明费马定理，我们从下列引理开始：

引理1 若$(a, m)=1$，则

$$a, 2a, 3a, \cdots, (m-1)a \tag{1}$$

的最小剩余$(\bmod m)$按某种次序排列后为

$$1, 2, 3, \cdots, m-1. \tag{2}$$

换一种不同的说法，就是：若$(a, m)=1$，则每一整数恰与$0, a, 2a, \cdots, (m-1)a$中之一同余$(\bmod m)$．例如，取$m=8$，$a=3$，则(1)中的数为

$$3, 6, 9, 12, 15, 18, 21,$$

而它们的最小剩余$(\bmod 8)$为

$$3, 6, 1, 4, 7, 2, 5.$$

引理1的证明 (1)中有$m-1$个数，与0都不同余$(\bmod m)$，因而它们中每一个应与(2)中一数同余$(\bmod m)$．如果我们能够证明(1)中任意两数互不同余，那就可推知它们的最小剩余$(\bmod m)$全不相同，因而就是$1, 2, \cdots, (m-1)$的一个重新排列．假定(1)中有两数同余$(\bmod m)$，即

$$ra \equiv sa (\bmod m);$$

由于$(a, m)=1$，我们可以消去a（§4定理4），而得

$$r \equiv s (\bmod m).$$

但r和s是对模m的最小剩余；根据我们以前数次用过的结论，可知$r=s$，引理得证．

费马定理的证明 给定任一素数p，引理1表明，若

$(a, p)=1$, 则

$$a,\ 2a,\ \cdots,\ (p-1)a$$

的最小剩余$(\bmod p)$是

$$1,\ 2,\ \cdots,\ p-1$$

的一个排列. 因此, 这两组数的乘积同余$(\bmod p)$:

$$a\cdot 2a\cdot 3a\cdot\cdots\cdot(p-1)a\equiv 1\cdot 2\cdot 3\cdot\cdots\cdot(p-1)(\bmod p),$$

也即 $$a^{p-1}(p-1)!\equiv(p-1)!(\bmod p).$$

由于p和$(p-1)!$互素, 由上一同余式可得

$$a^{p-1}\equiv 1(\bmod p),$$

这就是费马定理.

【练习 1】 当$a=2$, $p=5$时, 验证定理的正确性.

有时, 可用稍为不同的一种方式叙述费马定理:

推论 若p为素数, 则对一切a, 有

$$a^p\equiv a(\bmod p).$$

证明 若$(a, p)=1$, 由费马定理即可推出上式; 若$(a, p)=p$, 则上述推论便是$0\equiv 0(\bmod p)$, 它显然是正确的. 其它情况是不存在的.

作为一例, 我们来验证$3^{16}\equiv 1(\bmod 17)$. 没有必要去计算3^{16}这一很大的整数并用17相除: 我们可分阶段进行, 并同时按模17进行化约. 我们有

$$3^3\equiv 27\equiv 10(\bmod 17).$$

两边平方, 我们得

$$3^6\equiv 100\equiv -2(\bmod 17);$$

再次平方得$3^{12}\equiv 4(\bmod 17)$. 于是,

$$3^{16}\equiv 3^{12}\cdot 3^3\cdot 3\equiv 4\cdot 10\cdot 3\equiv 120\equiv 1(\bmod 17).$$

【练习 2】 计算2^5和$2^{10}(\bmod 11)$.

为了证明威尔逊定理, 我们需要两个引理.

引理2 $x^2\equiv 1 \pmod p$恰有两解：1和$p-1$.

证明 设r是$x^2\equiv 1 \pmod p$的任一解. 说到解，正如我们对线性同余式所说的一样，我们是指满足同余式的最小剩余. 那么$r^2-1\equiv 0 \pmod p$, 故

$$p \mid (r+1)(r-1).$$

因此，$p\mid(r+1)$或$p\mid(r-1)$; 换种方式表示就是,

$$r+1\equiv 0 \quad 或 \quad r-1\equiv 0 \pmod p,$$

故$r\equiv p-1$或$1 \pmod p$. 由于r是最小剩余$\pmod p$, 可得$r=p-1$或1. 容易验证，这两个数的确满足$x^2\equiv 1 \pmod p$.

引理3 假设p是一个奇素数，a'表示$ax\equiv 1 \pmod p$的解，$a=1, 2, \cdots, p-1$, 即$aa'\equiv 1 \pmod p$, 且$0\leqslant a'<p$. 那么，成立以下两个结论：

当$a\not\equiv b \pmod p$时，$a'\not\equiv b' \pmod p$;

仅当$a=1$或$a=p-1$时，$a'\equiv a \pmod p$.

证明 首先，我们注意到，由于$(a, p)=1$, $ax\equiv 1 \pmod p$恰有一解，故a'存在且是唯一的. 假定$a'\equiv b' \pmod p$, 则

$$1\equiv aa'\equiv ab' \pmod p,$$

即有

$$b\equiv ab'b\equiv a \pmod p,$$

这就证明了引理1的第一个结论. 为证第二个结论，假定

$$a\equiv a' \pmod p,$$

那么

$$1\equiv aa'\equiv a^2 \pmod p,$$

而由引理2我们知，仅当$a=1$或$a=p-1$时，这才有可能.

为了说明这一结果，让我们取$p=13$, 则有

a	1	2	3	4	5	6	7	8	9	10	11	12
a'	1	7	9	10	8	11	2	5	3	4	6	12
aa'	1	14	27	40	40	66	14	40	27	40	66	144

第二行中各数是第一行中各数的一个排列，每种情况下都有

$aa'\equiv 1 \pmod{13}$，而仅当 $a=1$ 或 12 时，有 $a\equiv a' \pmod{13}$。

威尔逊定理的证明 注意，$(2-1)!\equiv -1 \pmod 2$，因此，当 $p=2$ 时，定理成立。以下证明过程中，我们可假定 p 为奇素数。由引理 3 知，我们可将

$$2, 3, \cdots, p-2$$

分成 $(p-3)/2$ 对，并使每对由一整数 a 和它相应的 a' 组成，且 a' 不同于 a。例如，对于 $p=13$，这些数对是

$$(2, 7), (3, 9), (4, 10), (5, 8), (6, 11).$$

【练习 3】 当 $p=11$ 时，这种数对是哪些？

每对中的两个整数的乘积与 1 同余 $(\bmod\, p)$，故得

$$2\cdot 3\cdot\cdots\cdot(p-2)\equiv 1 \pmod p.$$

因此，

$$(p-1)!\equiv 1\cdot 2\cdot 3\cdot\cdots\cdot(p-2)(p-1)\equiv 1\cdot 1\cdot(p-1)$$
$$\equiv -1 \pmod p,$$

我们就证明了定理的一半。接下来要证另一半，即要说明，若

$$(n-1)!\equiv -1 \pmod n, \tag{3}$$

则 n 就是素数。假定对某两整数 a 和 b，$n=ab$，且 $a\neq n$。由 (3)，我们有

$$n\,|\,((n-1)!+1).$$

又因 $a\,|\,n$，我们有

$$a\,|\,((n-1)!+1). \tag{4}$$

但由于 $a\leqslant n-1$，可知 $(n-1)!$ 有一个因子就是 a 自身，因此，

$$a\,|\,(n-1)!. \tag{5}$$

但 (4) 和 (5) 说明，$a\,|\,1$，因而 n 可能有的因子只有 1 和 n，即 n 是素数。

【练习 4】 对于 $p=3, 5, 7$，验证

$$(p-1)!\equiv -1 \pmod p.$$

习　　题

1. 314^{159} 用 7 相除时，余数是什么?
2. 314^{162} 用 163 相除时，余数是什么?
3. 7^{355} 的末位数是什么?
4. 7^{355} 的末两位数是什么?
5. 对于 $r=1, 2, \cdots, p-1$，证明

$$(p-1)(p-2)\cdots(p-r)\equiv(-1)^r r!\pmod{p}.$$

6. 注意：$6!\equiv-1\pmod{7}$；　$5!1!\equiv1\pmod{7}$；$4!2!\equiv-1\pmod{7}$；
   $3!3!\equiv1\pmod{7}$.

   对模 11，试作同样的计算.
7. 根据习题 6 的数据，猜想一个定理，并证明之.
8. (a) 对 $n=4, 6, 8, 9, 10$，计算 $(n-1)!\pmod{n}$；
   (b) 猜想并证明一个定理.
9. 证明：若 p 为大于 5 的奇素数，则 $2(p-3)!+1\equiv0\pmod{p}$.
10. (a) 证明：若 $r!\equiv(-1)^r\pmod{p}$，则 $(p-r-1)!\equiv-1\pmod{p}$；
    (b) 举一个例子，找出这样的 p 和 r.
11. (a) 对 $k=0, 1, \cdots$，证明 $(k+1)^p-k^p\equiv1\pmod{p}$；
    (b) 由此推出费马定理.
12. 1732 年，欧拉(Euler)说道："我从一个优美的定理推出了某一结果，我虽不会证明它，但我肯定它是正确的：若 a 和 b 均不能被素数 $n+1$ 整除，则 a^n-b^n 可被 $n+1$ 整除."用费马定理证明这一定理.
13. 假定 p 是一个奇素数.
    (a) 证明：$1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv-1\pmod{p}$；
    (b) 证明：$1^p+2^p+\cdots+(p-1)^p\equiv0\pmod{p}$；
    (c) 证明：若 $2^m\not\equiv1\pmod{p}$，则

$$1^m+2^m+\cdots+(p-1)^m\equiv0\pmod{p}.$$

14. 有人证得下列定理：若 p 为素数，则对一切 a，有

$$a^p(p-1)!\equiv a(p-1)\pmod{p}.$$

证明由此定理可推得费马定理和威尔逊定理的一部分：

$$(p-1)!\equiv-1(\bmod p).$$

15. 计算 $2^{340}(\bmod 341)$，又知 $341=11\cdot31$，借此说明费马定理的逆命题不成立.
16. 满足 $n\mid(2^n-2)$ 的合数 n 称为**伪素数**. 存在着无限多个伪素数，最小的两个为 341 和 561. 验证 561 是一个伪素数.
17. 对一切 a 满足 $n\mid(a^n-a)$ 的合数 n 称为**绝对伪素数**. 最小的绝对伪素数为 561. 验证 $341\nmid(11^{341}-11)$，并借此说明 341 不是一个绝对伪素数.
18. 设 p 和 q 为任意两个不同的素数，证明:
    (a) 对一切 a，有 $pq\mid(a^{p+q}-a^{p+1}-a^{q+1}+a^2)$;
    (b) 对一切 a，有 $pq\mid(a^{pq}-a^p-a^q+a)$.
19. 证明: 若 p 是一个奇素数，则 $2p\mid(2^{2p-1}-2)$.
20. 若 p 是一个奇素数，$(a, p)=1$，则对模 p，$a^{(p-1)/2}$ 可取哪些值?
21. n 是什么数时，有 $p\mid(1+n+n^2+\cdots+n^{p-2})$?
22. 证明: 除 5 以外的所有奇素数均能整除形为 $111\cdots11$（k 位数，各位全为 1）的某一数.
23. 若 p 是一个奇素数，$(a, p)=1$，$n\mid(p-1)$，$a\equiv c^n(\bmod p)$，证明 $p\mid(a^{(p-1)/n}-1)$.

§7 整数的因子

这里，也许很自然地应讲讲二次同余式，以继续对同余式进行研究．但是，部分地出于使内容多样化的考虑，我们将先讨论一个不同的课题，以后再回过来研究同余式．

设 n 是一个正整数，$d(n)$ 表示 n 的正因子数（包括 1 和 n），$\sigma(n)$ 表示它们的和，即

$$d(n)=\sum_{d\mid n}1,\quad \sigma(n)=\sum_{d\mid n}d.$$

（你可能不熟悉这一求和记号，要是那样的话，可参阅附录二．）这些函数经常出现，本节中我们将推出它们的几个性质．在下节我们将用它们来研究完全数这一课题，它曾为古希腊数学家们所重视，以后也一直受到人们的注意．

【练习 1】 就下表已经列出的部分验证其正确性，并将此表完成之．

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$d(n)$	1	2	2	3	2	4	2	4	3	4						

若 p 是一个素数，则 $d(p)=2$，因为 p 的正因子只有 1 和 p．由于 p^2 具有因子 1，p 和 p^2，故 $d(p^2)=3$．

【练习 2】 $d(p^3)$ 是什么？推广至 $d(p^n)$，$n=4, 5, \cdots$．

若 $p\neq q$，则 pq 就有因子 1，p，q 和 pq，故 $d(pq)=4$．（本节中，和其它地方一样，p 和 q 将代表素数．）类似地，p^2q 的因子为 1，p，p^2，q，pq 和 p^2q，故 $d(p^2q)=6$．

【练习 3】 $d(p^3q)$ 是什么？对任意正整数 n，$d(p^nq)$ 是什

么？

做了练习 2 和练习 3，你可能已猜到

定理 1 若 $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ 是 n 的素数幂分解式（我们记得，对所有 i，有 $e_i\geqslant1$，且当 $i\neq j$ 时，$p_i\neq p_j$），则

$$d(n)=(e_1+1)(e_2+1)(e_3+1)\cdots(e_k+1).$$

如用比较简练的乘积记号写出，就有：若 $n=\prod_{i=1}^{k}p_i^{e_i}$，则 $d(n)=\prod_{i=1}^{k}(e_i+1)$；甚至还可写成：若 $n=\prod_{p|n}p^{a_p}$，则

$$d(n)=\prod_{p|n}(a_p+1).$$

证明 设 D 表示下列各数的集合：

(1) $$p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\quad（其中，0\leqslant f_i\leqslant e_i）.$$

我们断言，D 恰是 n 的各个因子组成的集合．首先，我们注意到，该集中任一数都是 n 的一个因子，这是因为，对于(1)中每个数，都能找到一个整数，即 $p_1^{e_1-f_1}p_2^{e_2-f_2}\cdots p_k^{e_k-f_k}$，它与那个数的乘积等于 n．其次，假设 d 是 n 的一个因子，若 $p|d$，则 $p|n$，故 d 的素数幂分解式中每一素数必在 n 的素数幂分解式中出现，因此，$d=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$，其中有些（或全部）指数可能为零．此外，任一指数 f_i 均不大于 e_i（不然的话，就会产生这样的情况，$p_i^{f_i}|d$，$d|n$，因而有 $p_i^{f_i}|n$，但因 $f_i>e_i$，这是不可能的）．于是，n 的每个因子都是集合 D 的一个元素．因此，D 等同于 n 的因子集合．

(1) 中每个 f_i 可取 e_i+1 个值，故在 D 中有

$$(e_1+1)(e_2+1)(e_3+1)\cdots(e_k+1)$$

个数，且由因子分解唯一性定理，它们全不相同，定理也就得证．

【练习 4】 计算 $d(240)$．

现在我们来为$\sigma(n)$找一个公式.

【练习 5】 就下表列出的部分验证此表的正确性，并完成此表：

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\sigma(n)$	1	3	4	7	6	12	8	15						

和$d(n)$一样，某些特殊的情况比较容易. 例如，对一切素数p，有$\sigma(p)=p+1$. 此外，p^2的因子为1，p和p^2，故

$$\sigma(p^2)=1+p+p^2=(p^3-1)/(p-1).$$

【练习 6】 $\sigma(p^3)$是什么？当p，q为不同的素数时，$\sigma(pq)$是什么？

【练习 7】 证明：$\sigma(2^n)=2^{n+1}-1$.

【练习 8】 $\sigma(p^n)$是什么？$n=1, 2, \cdots$.

当p，q为不同素数时，我们来计算$\sigma(p^eq^f)$，并看一看能否推想出一个一般性结果. p^eq^f的各个因子为

$$\begin{array}{lllll}
1, & p, & p^2, & \cdots, & p^e, \\
q, & pq, & p^2q, & \cdots, & p^eq, \\
q^2, & pq^2, & p^2q^2, & \cdots, & p^eq^2, \\
\cdots & \cdots & \cdots & \cdots & \cdots, \\
q^f, & pq^f, & p^2q^f, & \cdots, & p^eq^f.
\end{array}$$

如将它们逐行相加，可得

$$\begin{aligned}
\sigma(p^eq^f)&=(1+p+\cdots+p^e)+q(1+p+\cdots+p^e)\\
&\quad+q^2(1+p+\cdots+p^e)+\cdots+q^f(1+p+\cdots+p^e)\\
&=(1+q+\cdots+q^f)(1+p+\cdots+p^e).
\end{aligned}$$

再将几何级数相加，就有

$$\sigma(p^eq^f)=\frac{p^{e+1}-1}{p-1}\cdot\frac{q^{f+1}-1}{q-1}.$$

另外，$$\sigma(p^e)=\frac{p^{e+1}-1}{p-1}.$$

从以上两式可以推知下列定理：

定理 2 若 n 的素数幂分解式为 $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$，则

$$\sigma(n)=\frac{p_1^{e_1+1}-1}{p_1-1}\cdot\frac{p_2^{e_2+1}-1}{p_2-1}\cdots\frac{p_k^{e_k+1}-1}{p_k-1}. \tag{2}$$

证明 我们只需证明：n 的各因子之和为

$$(1+p_1+\cdots+p_1^{e_1})(1+p_2+\cdots+p_2^{e_2})\cdots(1+p_k+\cdots+p_k^{e_k}). \tag{3}$$

这是因为，(3) 与 (2) 的右端相等. 将 (3) 中各括号展开相乘得出的各项均为 k 个因子的乘积：一个因子来自第一个括号，一个因子来自第二个括号，如此等等，每一项的形式均为

$$p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k},$$

其中，$0\leqslant f_i\leqslant e_i$，$i=1,2,\cdots,k$. 但这些数正好就是 n 的全部因子.

【练习 9】 计算 $\sigma(240)$.

d 和 σ 这两个函数属于一类很重要的数论函数：积性函数. 现在我们就要定义这一术语，并验证 d 和 σ 都是积性函数，还要解释为什么这一概念非常重要. 一个定义在正整数集合上的函数，当且仅当由 $(m,n)=1$ 可得 $f(mn)=f(m)f(n)$ 时，我们称它为*积性函数*. $f(n)=n$ 就是一个积性函数的简单例子；$f(n)=n^2$ 也是一个积性函数.

定理 3 d 是积性函数.

证明 设 m 与 n 互素，那么，整除 m 的素数就不能整除 n，反之亦然. 因此，若

$$m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\qquad n=q_1^{f_1}q_2^{f_2}\cdots q_r^{f_r}$$

分别是 m 和 n 的素数幂分解式，则任一 q 都不是某个 p，任一 p 也都不是某个 q，由此可得 mn 的素数幂分解式：

$$mn = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}.$$

应用定理 1，我们有

$$d(mn) = ((e_1+1)(e_2+1)\cdots(e_k+1))((f_1+1)(f_2+1)$$
$$\cdots(f_r+1)) = d(m)d(n).$$

这就证明了定理.

定理 4 σ是积性函数.

证明 其思想与定理 3 的证明完全一样. 由m与n互素，如定理 3 那样，我们应用定理 2 可得

$$\sigma(mn) = \frac{p_1^{e_1+1}-1}{p_1-1} \cdots \frac{p_k^{e_k+1}-1}{p_k-1} \cdot \frac{q_1^{f_1+1}-1}{q_1-1} \cdots \frac{q_r^{f_r+1}-1}{q_r-1}$$
$$= \sigma(m)\sigma(n).$$

积性函数之所以重要，原因在于：如果我们知道了一个积性函数f在所有素数幂上的值，那么我们就能求出f在所有正整数上的值. 为了看出这一点，我们注意到下列定理：

定理 5 若f是一个积性函数，n的素数幂分解式为$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$，则

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k}).$$

证明 对k用归纳法来证. 当$k=1$时，不用说，定理成立. 假定定理对$k=r$成立. 由于

$$(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},\ p_{r+1}^{e_{r+1}}) = 1,$$

根据积性函数的定义，我们有

$$f((p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) p_{r+1}^{e_{r+1}}) = f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) f(p_{r+1}^{e_{r+1}}).$$

由归纳法假设，第一个因子为

$$f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_r^{e_r}),$$

此式和前一式并在一起就完成了归纳法证明.

例如，假定对一切素数p和所有数e，$e \geqslant 1$，有$f(p^e) = ep^{e-1}$，则f开头几个值为

n	2	3	4	5	6	7	8	9	10	11	12,
$f(n)$	1	1	4	1	1	1	12	6	1	1	4,

$$f(3141)=f(3^2\cdot 349)=f(3^2)f(349)=6\cdot 1=6.$$

类似地我们可对任一 n 算出 $f(n)$ 来.

【练习 10】 当 $n=13, 14, \cdots, 24$ 时，计算 $f(n)$.

在 § 9 中，我们将用定理 5 为一个重要的数论函数(即欧拉函数 ϕ)推出一个公式.

习 题

1. 计算: (a) $d(42)$; (b) $d(420)$; (c) $d(4200)$.
2. 计算: (a) $\sigma(42)$; (b) $\sigma(420)$; (c) $\sigma(4200)$.
3. 利用表 C 计算: (a) $d(10,001)$; (b) $d(10,008)$; (c) $d(100,001)$.
4. 利用表 C 计算: (a) $\sigma(10,001)$; (b) $\sigma(10,008)$; (c) $\sigma(100,001)$.
5. 1638 年，笛卡儿(Descartes)注意到，对于 $n=1, 2, \cdots$, 有
$$\sigma(p^n)-p^n=\frac{p^n-1}{p-1}.$$
验证这是正确的.
6. 卡达诺(Cardano)是提到 $d(n)$ 的第一个人. 1537 年，他说，若 $p_1, p_2, \cdots, p_k$ 是不同的素数，则
$$d(p_1p_2\cdots p_k)-1=1+2+2^2+\cdots+2^{k-1}.$$
验证这是正确的.
7. 证明: 若 n 是 2 的一个乘幂，则 $\sigma(n)$ 是奇数.
8. (a) 证明: 若 $f(n)$ 是积性函数，则 $f(n)/n$ 也是积性函数;
(b) 否定下列命题: 若 $f(n)$ 是积性函数，则 $f(n)-n$ 也是积性函数.
9. 使 $d(n)=8$ 的最小整数 n 是什么? 使 $d(n)=10$ 的最小整数 n 又是什么?
10. 当 k 为任一数时，$d(n)=k$ 是否对 n 都有解?
11. 1644 年，莫森(Mersenne)曾征求一个具有 60 个因子的数. 试在 10,000 以内求出这样一个数.

12．求出满足 $d(n)=60$ 的无限多个 n.

13．证明：$\sum_{d|n} 1/d=\sigma(n)/n$.

14．设 p 是一个奇素数，问 k 是什么数时，$1+p+\cdots+p^k$ 是奇数?

15．当 n 是哪些数时，$\sigma(n)$ 是奇数?

16．若 n 是一个平方数，证明 $d(n)$ 是奇数.

17．若 $d(n)$ 是奇数，证明 n 是一个平方数.

18．求 $1/x+1/y=1/6$ 的所有 17 组整数解(正整数或负整数).

19．对一给定的正整数 N，$1/x+1/y=1/N$ 有多少组解?

20．对 k 用归纳法证明定理 2.

21．求无限多个 n 使 $\sigma(n)\leqslant\sigma(n-1)$.

22．若 N 为奇数，$x^2-y^2=N$ 有多少组解?

23．若 N 为奇数，证明 $x^2-y^2=2N$ 无解.

24．记 $\sigma_2(n)$ 是 n 的正因子的平方和，为它推出一个公式.

25．记 $\sigma_k(n)=\sum_{d|n} d^k$，其中 k 为正整数. 为它猜想一个公式.

26．证明 n 的正因子乘积为 $n^{d(n)/2}$.

§8 完 全 数

当且仅当一个数等于除它自身以外的各个正因子之和时，这个数称为完全数. 例如，6 是完全数，因为 $6=1+2+3$; 28 也是完全数，因为 $28=1+2+4+7+14$; 但 18 不是完全数，因为除了它自身以外的各个正因子之和是

$$1+2+3+6+9=21.$$

我们所以要研究完全数，一方面是因为，在过去，出于某些令人费解的原因，许多人曾经非常注意这些数；另一方面也因为，这些数为 σ 函数提供了练习的机会；然而最重要的还是因为，欧拉曾证得了一个令人满意的定理，它使我们能够求出所有的偶完全数. 在欧拉以前很久，欧几里得就发现了若干完全数. 我们将顺着他的路子走下去.

n 除了它自身外的所有正因子之和，用符号表示即为 $\sigma(n)-n$，因此，一个数为完全数的充要条件是 $\sigma(n)=2n$. 为了求解这一方程，我们要用到§7中证明的一个结果，即 σ 是一个积性函数，也就是

(1) $\qquad (m, n)=1$ 时，$\quad \sigma(mn)=\sigma(m)\sigma(n)$.

借助于这一结果，我们可证明

定理 1（欧几里得） 若 2^p-1 为素数，则 $2^{p-1}(2^p-1)$ 是完全数.

证明 设 $n=2^{p-1}(2^p-1)$. 由于 2^p-1 是素数，我们知，$\sigma(2^p-1)=2^p$. 那么，注意到 2^{p-1} 和 2^p-1 是互素的并利用(1)，我们有

$$\sigma(n)=\sigma(2^{p-1}(2^p-1))=\sigma(2^{p-1})\sigma(2^p-1)$$
$$=(2^p-1)\cdot 2^p=2n.$$

故 n 是完全数.

如果你做过 § 2 的题 13，你也许已经发现，当 n 为合数时，2^n-1 也是合数(因为，若 $n=ab$，则

$$2^n-1=2^{ab}-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\cdots+1).$$

故仅当 n 为素数时，2^n-1 才有可能是素数. 因此，为了寻找形为 $2^{n-1}(2^n-1)$ 的完全数，我们只需考虑 n 为素数的情况即可，而每当我们找到一个素数，它使 2^p-1 也是一个素数，我们就能造出一个完全数. 2^p-1 的开头几个数值由下表给出：

p	2	3	5	7	11	13
2^p-1	3	7	31	127	2047	8191.

这些数中，除 $2047=23\cdot 89$ 外，均为素数，因而我们找到了五个完全数：

$$2(2^2-1)=6,$$
$$2^2(2^3-1)=28,$$
$$2^4(2^5-1)=496,$$
$$2^6(2^7-1)=8128,$$
$$2^{12}(2^{13}-1)=33550336.$$

下面是一个较大的完全数：

191561942608236107294793378084303638130993721548169216.

现在我们将证明，p 和 2^p-1 均为素数时的数 $2^{p-1}(2^p-1)$ 是仅有的偶完全数.

定理 2(欧拉) 若 n 是一个偶完全数，则

$$n=2^{p-1}(2^p-1),$$

其中 p 为某素数，且 2^p-1 也是素数.

证明 若 n 为偶完全数，则 $n=2^e m$，其中 m 是奇数，且

$e \geqslant 1$. 由于 $\sigma(m)>m$, 我们可记 $\sigma(m)=m+s$, 其中 $s>0$. 于是, $2n=\sigma(n)$ 就成为

$$2^{e+1}m=(2^{e+1}-1)(m+s)=2^{e+1}m-m+(2^{e+1}-1)s.$$

因此,

(2) $$m=(2^{e+1}-1)s.$$

此式说明, s 是 m 的一个因子, $s<m$. 但 $\sigma(m)=m+s$, 因而 s 是 m 的所有小于 m 的因子之和, 也就是说, s 是包括 s 在内的一组数之和. 仅当这组数只包含一个数时这才是可能的. 因此, m 的小于 m 的因子的集合只包含一个元素, 那个元素必定为 1, 即 $s=1$, 故 $m=2^{e+1}-1$ 是一个素数.

鉴于这一论证非常巧妙, 我们要重复一下. 设 m 的因子为

$$1,\ d_2,\ d_3,\ \cdots,\ d_k,\ m,$$

则 $\sigma(m)=m+s$, 其中

$$s=1+d_2+d_3+\cdots+d_k.$$

但 s 是 m 的一个因子, $s<m$, 故 s 等于 1, d_2, $\cdots$, d_k 中之一, 唯一可能的是 $s=1$.

我们已经表明, $s=1$, 因此 $\sigma(m)=m+s=m+1$, 这就说明了 m 是素数. 由(2), $m=2^{e+1}-1$. 具有这种形式的数要是素数, 只有 $e+1$ 是素数才行, 因此 $m=2^p-1$, p 为某一素数, 证毕.

这样, 由定理 1 得出的偶完全数就是全部偶完全数. 至于奇完全数, 谁也不知道它们是否存在, 也没有人证明过它们不可能存在. 要是存在一个奇完全数的话, 那么它一定是非常大的: 1967 年, 有人宣布, 它必须大于 10^{36}, 而且奇完全数还必须满足许多其它条件. 但是, 到目前为止, 还没有凑出这样的条件, 可以用来说明不存在奇完全数. 奇完全数也许会

有，但它实在太大，以致超出了人们能够计算的范围.

介绍了定理 2，求偶完全数的问题就等同于求素数 p 使 2^p-1 也为素数的问题了. 形为 2^p-1 的素数叫做莫森数. 在十七世纪的时候，莫森(Mersenne)声称，当 $p=2, 3, 5, 7, 13, 17, 31, 67, 127, 257$ 时，2^p-1 是素数，对于 257 以下的其它素数 p，2^p-1 均非素数. 他这一猜想是不准确的：他将 67 和 257 包括在内是不对的，因为

$$2^{67}-1=193707721\cdot761838257287,$$

$2^{257}-1$ 也是合数；另外，他把 19, 61, 89, 107 排除在外也错了. 当然，对莫森可别太苛刻了：在十七世纪，还没有任何数学刊物来宣布新的发现；几乎所有人都把最新的数学消息写信告诉莫森，而莫森也把这些消息写信告诉其他人，因此，他传播了费马等人的成果，加速了数学的发展. 所以，有一类素数以他的名字来命名，这还是合适的. 目前已经知道的能使 2^p-1 也为素数的所有素数 p 是：

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127,
521, 607, 1279, 2203, 2281, 3217, 4253,
4423, 9689, 9941, 11213.

这些数中每一个都对应着一个偶完全数：一共是 23 个. 前面 12 个是在高速计算机发明以前发现的，后面 11 个实在太大了，用手来计算已经办不到. 人们继续在寻找莫森素数(上面最后几个数就是新近发现的)，希望能看出素数 p 的形式，以便能够猜想并证明一些定理. 有人已经提出了一些猜想，但还没有迹象表明如何着手证明它们. 事实上，还没有证得任何重要的定理，甚至还不清楚是否一定存在无限多个这样的素数.

在结束本节时，我们还要提一提另一类曾使一些人颇感

兴趣的数：亲和数．考虑220和284．因$220=2^2\cdot5\cdot11$，可知

$$\sigma(220)-220=\sigma(2^2)\sigma(5)\sigma(11)-220$$
$$=7\cdot6\cdot12-220=504-220=284.$$

又因$284=2^2\cdot71$，我们有

$$\sigma(284)-284=\sigma(2^2)\sigma(71)-284=7\cdot72-284$$
$$=220.$$

所以，在某种意义上说，220和284一起出现．一般地，当且仅当

$$\sigma(m)-m=n \quad 且 \quad \sigma(n)-n=m$$

时，我们称m和n是亲和数(或一对亲和数)．换一种等价的说法，就是：当且仅当$\sigma(m)=\sigma(n)=m+n$时，m和n是亲和数．

【练习1】 验证1184和1210是亲和数．

亲和数直到二十世纪初还得到一些受人尊敬的数学家的注意(练习1中这对亲和数直到1866年才被发现)；欧拉发现了许多对亲和数．有一长串亲和数存在(除了前面已经提到的亲和数外，10,000以内的亲和数还有三对：2620，2924；5020，5564；6232，6368)．但是，关于完全数的欧几里得定理和欧拉定理那样漂亮的一般性定理，对于亲和数却尚未找到．如今，亲和数已不很受到人们的重视，我们将它们以及其它类似的数放到下面习题中去讨论．

习　　题

1. 验证：$17296=2^4\cdot23\cdot47$和$18416=2^4\cdot1151$是亲和数．(这一对是费马发现的，也是220，284那一对以后发现的第一对，而220，284这一对古希腊人就已经知道．)
2. 过去曾长期有人认为，偶完全数交替地以6和8结尾，说明这是错误的，并验证

$$2^{12}(2^{13}-1) \equiv 2^{16}(2^{17}-1) \equiv 6 \pmod{10}.$$

3. 1575 年,有人注意到,每个偶完全数也是一个三角形数,证明这是正确的.

4. 1652 年,有人注意到,

$$6=1+2+3,$$
$$28=1+2+3+4+5+6+7,$$
$$496=1+2+3+\cdots+31,$$

这类式子还能继续写下去吗?

5. 证明:若 m 和 n 为亲和数,则

$$\sum_{d\mid m} d=\sum_{d\mid n} d=m+n.$$

6. 证明:若 m 和 n 为亲和数,则

$$\Big(\sum_{d\mid m} 1/d\Big)^{-1}+\Big(\sum_{d\mid n} 1/d\Big)^{-1}=1.$$

7. 设:$p=3\cdot 2^{e}-1$,
$q=3\cdot 2^{e-1}-1$,
$r=3\cdot 2^{2e-1}-1$,

其中 e 是一个正整数. 若 p, q 和 r 均为素数,证明 $2^{e}pq$ 和 $2^{e}r$ 是亲和数.($e=2, 4, 7$ 时,能够得到亲和数,但对 $e\leqslant 200$ 的其它数,都不会使 p, q, r 均为素数.)

8. 证明:任一素数都不会成为某对亲和数中之一数.

9. 若 p^{e} 是一对亲和数中之一数,证明

$$\sigma(p^{e})=\sigma\left(\frac{p^{e}-1}{p-1}\right).$$

10. (a) 证明:$\sigma(1+p)<1+p+p^{2}$;

(b) 用上式证明:p^{2} 决不会是一对亲和数中之一数.

11. 若 $\sigma(n)=kn$,则 n 被称为 k **类完全数**. 验证 672 是 3 类完全数,$2,178,540=2^{2}\cdot 3^{2}\cdot 5\cdot 7^{2}\cdot 13\cdot 19$ 是 4 类完全数.

12. 设 $s(n)=\sigma(n)-2n$. 若 $s(n)=0$,则 n 是完全数;若 $s(n)>0$,我们称 n 是**过剩数**;若 $s(n)<0$,我们称 n 是**亏缺数**.

(a) 验证 12 和 24 是过剩数,8 和 14 是亏缺数;

(b) 将小于或等于 20 的正整数分类成过剩数、亏缺数和完全数.

(c) 过去曾长期认为，每一过剩数均为偶数. 证明 945 是过剩数;

(d) 证明: 当 $n=3, 4, 5, 6, 7, 8, 9$ 时, $n(n+1)$是过剩数; 而当 $n=10$ 时, $n(n+1)$ 是亏缺数;

(e) 若 $p>3$, 且 $2p+1$ 为素数, 证明 $2p(2p+1)$是亏缺数. 事实上, $s(2p(2p+1))=-2p^2+8p+6$;

(f) 证明 $pq(pq\neq6)$是亏缺数;

(g) 设 $n=2^k(2^{k+1}-1)$. 若 $2^{k+1}-1$ 为合数, 证明 n 是过剩数;

(h) 若 $n=2^k(2^{k+1}-1)$是完全数, 且 $d|n$, $1<d<n$, 证明 d 是亏缺数;

(i) 若 $n=2^k(2^{k+1}-1)$是完全数, 且 $p<2^{k+1}-1$ 为素数, 证明 2^kp 是过剩数.

13. 证明: p^e(p 为大于 2 的素数, $e\geqslant1$)是亏缺数.

14. 证明所有的偶完全数以 6 或 8 结尾.

15. 若 n 为偶完全数, $n>6$, 证明 $n\equiv1 \pmod 9$.

16. 证明: 若 p 为奇数, 则

$$2^{p-1}(2^p-1)\equiv1+9\binom{p}{2} \pmod{81}.$$

(关于记号$\binom{m}{n}$, 参见附录二.)

17. 欧拉曾证明, 任何奇完全数的形式必为 $p^{4a+1}Q^2$, 其中 p 为奇素数, a 和 Q 为整数. 在他的证明的草稿上补进未详细写出的内容:

设 $n=P_1P_2\cdots P_k$ 是将 n 分解为不同奇素数幂的表示式. 令 $Q_i=\sigma(P_i)$, $i=1, 2, \cdots, k$. 若 $\sigma(n)=2n$, 则

$$2P_1P_2\cdots P_k=Q_1Q_2\cdots Q_k.$$

因此, $Q_1, Q_2, \cdots, Q_k$ 中有一数, 比方说是 Q_1, 是一个奇素数的 2 倍, 而其余各数均为奇数. 故 $P_2, P_3, \cdots, P_k$ 是素数的偶次幂, 而 $P_1=p^{4a+1}$, p 为某素数, a 为某整数.

18. 下面是欧拉对定理 2 作出的原来的证明, 补上所有未详细写出的内容:

设 $n=2^km$ 是完全数, m 为奇数. n 的各因子之和$(2^{k+1}-1)\sigma(m)$ 应等于 $2n$. 因而

$$m/\sigma(m)=(2^{k+1}-1)/2^{k+1},$$

它是一个既约分数．因此，对某整数 c，有 $m=(2^{k+1}-1)c$．若 $c=1$，则 $m=2^{k+1}-1$ 必为素数，因为 $\sigma(m)=2^{k+1}$；若 $c>1$，则

$$\sigma(m)\geqslant m+(2^{k+1}-1)+c+1.$$

于是，
$$\frac{\sigma(m)}{m}\geqslant\frac{2^{k+1}(c+1)}{m}>\frac{2^{k+1}}{2^{k+1}-1},$$

出现矛盾．

§9 欧拉定理和欧拉函数

费马定理称:

若$(a, p)=1$,则

$$a^{p-1}\equiv 1 \pmod p.$$

很自然地要问，能不能将它推广到模为合数的情形？给定任一整数 m,是否存在一数 $f(m)$,使 $a^{f(m)}\equiv 1 \pmod m$？我们知道,除非$(a, m)=1$,否则这是不可能成立的，因为，若 a 和 m 有大于 1 的公因子,那么对任一 $k>0$，不可能有 $m\mid(a^k-1)$. 让我们看一下几张 a 的乘幂 $(\bmod m)$表，其中 a 与 m 互素，$m=6, 9, 10$:

$m=6$

a	a^2
1	1
5	1

$m=9$

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	7	4	1
8	1	8	1	8	1

$m=10$

a	a^2	a^3	a^4
1	1	1	1
3	9	7	1
7	9	3	1
9	1	9	1

显然,

若$(a, 6)=1$,则

$$a^2\equiv 1 \pmod 6;$$

若$(a, 9)=1$,则

$$a^6\equiv 1 \pmod 9;$$

若$(a, 10)=1$,则

$$a^4 \equiv 1 \pmod{10}.$$

所以,对于$m=6, 9, 10$,数$f(m)$是存在的.

【练习1】 证明:对所有与14互素的a,有

$$a^6 \equiv 1 \pmod{14}.$$

要是你目光真的敏锐,你就可能已经注意到,$f(6)=2$,同时恰有2个小于6且与6互素的正整数;$f(9)=6$,同时恰有6个小于9且与9互素的正整数;$f(10)=4$,同时恰有4个小于10且与10互素的正整数;对于14,类似的说法也成立.因此,你可以猜出下列定理(要是你研究了更多的例子,就几乎一定能将它猜出来的):

定理1 设$m \geqslant 2$,且$(a, m)=1$.若$\phi(m)$表示小于m且与m互素的正整数个数,则

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

注意,在$m=p$是一素数这个特殊情况下,上述猜想是正确的,因为小于p的每个正整数都与p互素,故$\phi(p)=p-1$,而我们知道,当$(a, p)=1$时,$a^{p-1} \equiv 1 \pmod{p}$.

我们在这一节里将要证明定理1,还要根据n的素数幂分解式导出一个计算$\phi(n)$的公式.定理1首先由欧拉证得,故ϕ就称作欧拉函数.

证明费马定理时的想法是:若$(a, p)=1$,则$a, 2a, \cdots, (p-1)a$的最小剩余$\pmod{p}$是$1, 2, \cdots, p-1$的一个排列.这一想法也是欧拉进行推广的关键:

引理1 若$(a, m)=1$,$r_1, r_2, \cdots, r_{\phi(m)}$是小于$m$且与$m$互素的正整数,则

(1) $$ar_1, ar_2, \cdots, ar_{\phi(m)}$$

的最小剩余$\pmod{m}$是

$$r_1, r_2, \cdots, r_{\phi(m)}$$

的一个排列.

【练习 2】 若 $m=10$, $a=3$, 验证引理 1 的正确性.

引理 1 的证明 由于集合(1)中恰有 $\phi(m)$ 个数, 要证它们的最小剩余是 $r_1, r_2, \cdots, r_{\phi(m)}$ 这 $\phi(m)$ 个数的一个排列, 我们必须说明, 它们互不相同, 且都与 m 互素. 为了说明它们互不相同, 可设对某 i 和 j $(1\leqslant i\leqslant\phi(m), 1\leqslant j\leqslant\phi(m))$, 有

$$ar_i\equiv ar_j \pmod m.$$

由于 $(a, m)=1$, 我们可从同余式两边消去 a 而得

$$r_i\equiv r_j \pmod m.$$

又因 r_i 和 r_j 都是最小剩余 $(\bmod m)$, 可得 $r_i=r_j$. 因此, 由 $r_i\neq r_j$, 可得 $ar_i\not\equiv ar_j \pmod m$, 故(1)中各数互不相同.

为了证明(1)中各数都与 m 互素, 可假定 p 是 m 和某个 ar_i 的公共素因子, 其中 $1\leqslant i\leqslant\phi(m)$. 因 p 是素数, 故有 $p\mid a$ 或 $p\mid r_i$. 因此, p 或为 a 和 m 的公因子, 或为 r_i 和 m 的公因子. 但 $(a, m)=(r_i, m)=1$, 故两种情况均不可能, 因而对每个 i, $i=1, 2, \cdots, \phi(m)$, 都有 $(ar_i, m)=1$.

欧拉定理的证明与费马定理的证明相似.

定理 1 的证明 由引理 1, 我们知

$$\begin{aligned} r_1r_2\cdots r_{\phi(m)} &\equiv (ar_1)(ar_2)\cdots(ar_{\phi(m)}) \\ &\equiv a^{\phi(m)}(r_1r_2\cdots r_{\phi(m)}) \pmod m. \end{aligned}$$

由于 $r_1, r_2, \cdots, r_{\phi(m)}$ 中每一个数都与 m 互素, 所以它们的乘积也与 m 互素, 于是这个乘积因子就可从上述同余式中消去, 我们便得

$$1\equiv a^{\phi(m)} \pmod m.$$

本节的其余部分将主要用于研究 ϕ 的性质. 我们的目标是用一种方法找出计算 $\phi(n)$ 的途径, 而且用不着去实际求出

小于 n 且与 n 互素的所有正整数.

【练习 3】 验证下表列出的数是正确的:

n	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	2	2	4	2	6	4	6	4.

为了使 $\phi(n)$ 对一切正整数都存在, 我们规定 $\phi(1)$ 就是 1. 有了这一规定, 定理 1 就对所有正整数 m 成立.

【练习 4】 验证 $3^{\phi(8)}\equiv 1 \pmod 8$. $\phi(8)=4$ $3^4=81\equiv 1 \pmod 8$

【练习 5】 哪些数小于 4 并与 4 互素?用 8 和 16 代替 4, 答案是什么? 你能为 $\phi(2^n)$ $(n=1, 2, \cdots)$ 推出一个公式吗?

一般地, 要看出 $\phi(p^n)$ 是什么并不难, 这里 p 是素数, n 是正整数.

引理 2 对一切正整数 n, 有 $\phi(p^n)=p^{n-1}(p-1)$.

证明 小于或等于 p^n 且与 p^n 不互素的正整数恰是 p 的各个倍数:

$$1\cdot p,\ 2\cdot p,\ 3\cdot p,\ \cdots,\ (p^{n-1})p,$$

它们一共有 p^{n-1} 个. 而小于或等于 p^n 的正整数总共有 p^n 个, 故我们有

$$\phi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1).$$

【练习 6】 验证此公式对于 $p=n=3$ 是正确的.

于是, 我们对所有素数幂的 ϕ 都已求得. 要是我们还知道 ϕ 是一个积性函数的话, 那么我们就可用 §7 定理 5 求得 $\phi(n)$ 的一个公式. 我们将用一个定理来表明 ϕ 确实是一个积性函数. 这个定理的证明, 与数论中其它许多证明一样, 既不长且不偏, 也不复杂, 就是困难一些. 我们首先需要一个容易的引理:

引理 3 若 $(a, m)=1$, 且 $a\equiv b \pmod m$, 则 $(b, m)=1$.

证明 因对某 k, 有 $b=a+km$, 引理即可得证.

推论 若

(2) $$r_1,\ r_2,\ \cdots,\ r_m$$

的最小剩余(mod m)是0, 1, …, $m-1$的一个排列, 则(2)中恰有$\phi(m)$个元素与m互素.

我们现在就能证明

定理2 ϕ是积性函数.

证明 我们将1到mn各数写出如下:

$$\begin{matrix} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ & \cdots & & \cdots & \\ m & 2m & 3m & \cdots & mn. \end{matrix}$$

假定$(m,\ r)=d$, 且$d>1$, 则我们可说, 在此表第r行

$$r \quad m+r \quad 2m+r \quad \cdots \quad (n-1)m+r$$

中, 任一元素都不与mn互素. 这是因为, 由$d|m$, $d|r$, 知$d|mn$, 且对任一k有$d|(km+r)$. 所以, 如果我们要找与mn互素的数, 除了第一个元素是与m互素的那些行以外, 在其它各行就一个也找不到.

【练习7】 上表中有多少行其第一个元素与m互素?

让我们举一个例子, 取$n=5$, $m=6$, 就有下表:

1	7	13	19	25
2	8	14	20	26
3	9	15	21	27
4	10	16	22	28
5	11	17	23	29
6	12	18	24	30.

第2、3、4、6各行没有元素与$mn=30$互素, 因为这些行的第一个元素都不与$m=6$互素. 所有与30互素的数都在余下

的两行中可以找到：

$$\begin{matrix} 1 & 7 & 13 & 19 & 25 \\ 5 & 11 & 17 & 23 & 29. \end{matrix}$$

假定我们能够证明，第一个元素与m互素的各行中，每行恰有$\phi(n)$个数与mn互素，而由于这种行共有$\phi(m)$行，可知整个表中与mn互素的数共有$\phi(n)\phi(m)$个，也即$(m, n)=1$时，$\phi(mn)=\phi(m)\phi(n)$，定理即可得证．但第r行(r与m互素)中各数为

(3) $$r,\ m+r,\ 2m+r,\ \cdots,\ (n-1)m+r,$$

而且我们可说，它们的最小剩余$(\bmod n)$是

(4) $$0,\ 1,\ 2,\ \cdots,\ n-1$$

的一个排列．为了验证这一论断，我们只需证明，(3)中任何两数均不同余$(\bmod n)$，因为(3)和(4)都只有n个元素．但这是很容易的：假定

$$km+r\equiv jm+r\ (\bmod n),$$

其中$0\leqslant k<n, 0\leqslant j<n$，就有$km=jm\ (\bmod n)$．而由于$(m, n)=1$，我们得$k\equiv j\ (\bmod n)$．考虑到$k$和$j$所满足的上述不等式，可得$k=j$．因此，若$k\neq j$，就有$km+r\not\equiv jm+r\ (\bmod n)$，故(3)中任何两个元素互不同余$(\bmod n)$．

根据引理3的推论，我们知(3)中恰有$\phi(n)$个元素与n互素．但由引理3，表中第r行中每一元素都与m互素，因此，该行恰有$\phi(n)$个元素与mn互素．正如我们前面已经提到，有了这一点，定理的证明也就完成了．

在前面的例子中，包含着与30互素的全部元素的那两行中各数的最小剩余(mod 5)为

$$\begin{matrix} 1 & 2 & 3 & 4 & 0; \\ 0 & 1 & 2 & 3 & 4, \end{matrix}$$

每一行都含有 $\phi(5)=4$ 个与 30 互素的数,因此

$$8=\phi(30)=\phi(6)\phi(5).$$

现在我们就能求得 $\phi(n)$ 的一个公式了:

定理 3 若 n 的素数幂分解式为 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$,则

$$\phi(n)=p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k-1}(p_k-1).$$

证明 由于 ϕ 是积性函数,用 §7 定理 5 可得

$$\phi(n)=\phi(p_1^{e_1})\phi(p_2^{e_2})\cdots\phi(p_k^{e_k}).$$

若对右端各个因子应用引理 2,定理即可得证.

【练习 8】 用定理 3 计算 $\phi(72)$, $\phi(74)$, $\phi(76)$.

定理 3 的公式可用另一更为简洁有用的形式写出:

推论 若 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$,则

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

这一推论的证明留给读者.

我们用下一节所需要的一个定理来结束本节.

【练习 9】 对下列各个 n, 分别计算 $\sum_{d\mid n}\phi(d)$:

(a) $n=12, 13, 14, 15, 16$;

(b) $n=2^k$, $k\geqslant1$;

(c) $n=p^k$, $k\geqslant1$, p 为奇素数.

现在你应该猜想到下列定理的正确性.

定理 4 若 $n\geqslant1$,则

$$\sum_{d\mid n}\phi(d)=n.$$

证明 很自然地我们会试图用定理 3 的公式来得出这一结果,但这将非常困难;我们还是用高斯首次提出的一个巧妙想法吧. 考虑整数 $1, 2, \cdots, n$. 对这些整数中的一个数,当且仅当它与 n 的最大公因子为 d 时,我们将它归入类 C_d 中. 例如,若 $n=12$,我们有

$$C_1=\{1,\ 5,\ 7,\ 11\},\quad C_2=\{2,\ 10\},\quad C_3=\{3,\ 9\},$$
$$C_4=\{4,\ 8\},\quad C_6=\{6\},\quad C_{12}=\{12\}.$$

【练习 10】 当 $n=14$ 时，各类 C_d 是什么？

当且仅当 $(m,\ n)=d$，即 $(m/d,\ n/d)=1$ 时，m 属于 C_d. 因此，根据欧拉函数 ϕ 的定义，类 C_d 中元素个数为 $\phi(n/d)$.

【练习 11】 对 $n=12$ 和 $n=14$，验证这一结论的正确性.

对应于 n 的每一因子 d，都存在着一类 C_d，因此，各类 C_d 的所有元素合在一起后，总数即为

$$\sum_{d|n}\phi(n/d).$$

但由于在 1, 2, …, n 这些整数中，每一个恰属于一类，故这个数正好就是 n，即有

$$n=\sum_{d|n}\phi(n/d)=\sum_{d|n}\phi(d)$$

定理得证.

习 题

1. 计算：$\phi(42)$, $\phi(420)$, $\phi(4200)$.
2. 计算：$\phi(10,001)$, $\phi(100,001)$.
3. 验证：若 $(a,\ 15)=1$，则 $a^8\equiv1\ (\mathrm{mod}\ 15)$.
4. 小于 18 且与 18 互素的正整数是哪些？当 $m=18$, $a=5$ 时，验证引理 1 是正确的.
5. 完全数满足 $\sigma(n)=2n$，什么数满足 $\phi(n)=2n$？
6. 证明：若 n 为奇数，则 $\phi(4n)=2\phi(n)$.
7. $1+2=(3/2)\phi(3)$, $1+3=(4/2)\phi(4)$, $1+2+3+4=(5/2)\phi(5)$, $1+5=(6/2)\phi(6)$, $1+2+3+4+5+6=(7/2)\phi(7)$, $1+3+5+7=(8/2)\phi(8)$. 推想一个定理.
8. 证明：$\sum_{p\leq x}\sigma(p)-\sum_{p\leq x}\phi(p)=\sum_{p\leq x}d(p)$.
9. 利用下列性质：总有整数 r 和 s 使 $ar+ms=1$，证明引理 3.
10. 若 $(a,\ m)=1$，证明：任一使 $x\equiv ca^{\phi(m)-1}\ (\mathrm{mod}\ m)$ 成立的 x 也满足

$$ax \equiv c \pmod{m}.$$

11. (a) 若 p 为奇素数,下列序列中有多少个元素与 p 互素?

$$1\cdot 2,\ 2\cdot 3,\ 3\cdot 4,\ \cdots,\ p(p+1);$$

(b) 若 p 为奇素数,下列序列中有多少个元素与 p 互素?

$$1\cdot 2,\ 2\cdot 3,\ 3\cdot 4,\ \cdots,\ p^2(p^2+1);$$

(c) 可以猜想一个一般性定理吗?

12. 求 $\phi(n)=16$的四个解.

13. 设 $n=dm$, 证明小于 n 且与 n 的最大公因子为 d 的正整数一共有 $\phi(m)$个.

14. 证明: 若m和n有一个大于1的公因子, 则 $\phi(mn)>\phi(m)\phi(n)$.

15. 设 $\phi^{(2)}(n)=\phi(\phi(n))$, $\phi^{(3)}(n)=\phi(\phi^{(2)}(n))$, 如此等等. 又设 $e(n)$ 是满足 $\phi^{(e(n))}(n)=2$ 的最小整数,对下列 n 计算 $e(n)$:

(a) $n=3, 4, 5, 6, 7, 8, 9$;

(b) $n=2^k$, $k\geqslant 2$;

(c) $n=3^k$, $k\geqslant 1$;

(d) $n=2^k3^j$, $k\geqslant 1$, $j\geqslant 1$.

16. 证明: 若$(m, n)=2$,则 $\phi(mn)=2\phi(m)\phi(n)$.

17. 若$(m, n)=p$,则 $\phi(mn)$与 $\phi(m)\phi(n)$间有什么关系?

18. 证明: 当且仅当对某正整数 k 有 $n=2^k$ 时,$\phi(n)=n/2$.

19. 证明: 当且仅当对某两正整数 k 和 j 有 $n=2^k3^j$ 时, $\phi(n)=n/3$.

20. 证明: 若 $6|n$,则 $\phi(n)\leqslant n/3$.

21. 证明: 若$n-1$ 和 $n+1$ 均为素数,且 $n>4$,则 $\phi(n)\leqslant n/3$.

22. 假设我们已知:

若 $p|n$,则 $\phi(np)=p\phi(n)$;

若 $p\nmid n$,则 $\phi(np)=(p-1)\phi(n)$,

利用它们推出 $\phi(n)$ 的公式.

23. 对下列 n 计算 $\sum\limits_{d|n}(-1)^{n/d}\phi(d)$:

(a) $n=12, 13, 14, 15, 16$;

(b) $n=p$, p 为奇素数;

(c) $n=2^k$, $k\geqslant 1$;

(d) $n=p^k$, $k\geqslant 1$, p 为奇素数;

(e) 猜想一个定理.

24．求出满足 $4\nmid\phi(n)$ 的所有 n.

25．证明：$\phi(n)=14$ 是不可能成立的.

26．求出一个正整数 k, $k\neq 7$, 使 $\phi(n)=2k$ 不可能成立.

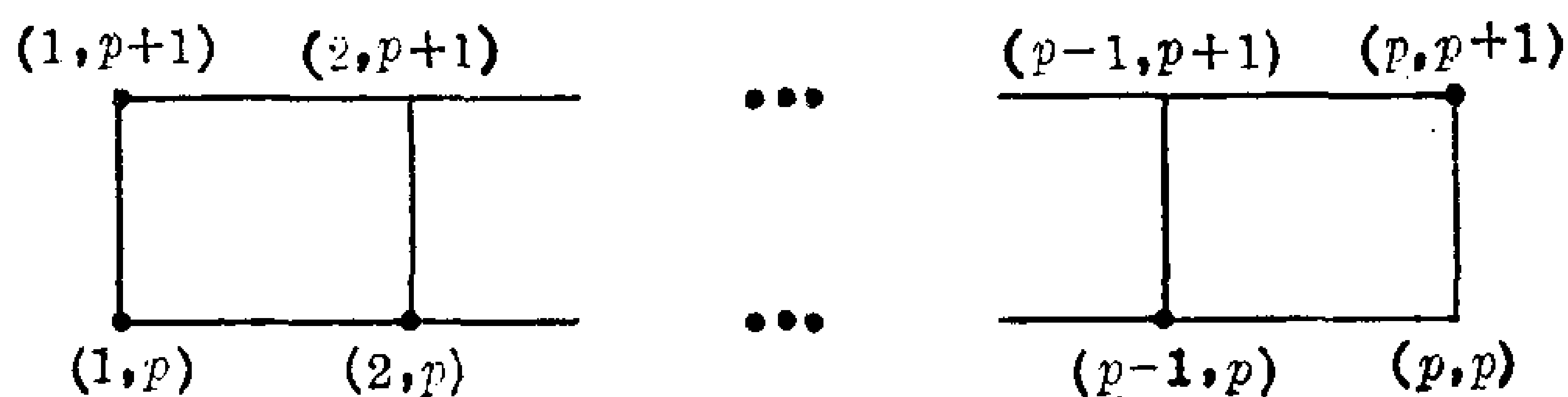
27．证明题 7 之定理.

28．在一个直角坐标系中，当且仅当 n 和 m 互素时，在点 (n, m) 处打上一个点. 考虑挨次排列着的一些方格.

(a) 有没有这样的方格，它的四只角都打上了点?

(b) 找出一个方格，它的四只角均未打点;

(c) 设 p 为奇素数，在下列一行方格中:



有多少个方格在三只角上打了点?

§10 原根和指数

从上节定理1我们已经看到：若$(a,\ m)=1$，则存在着正整数t使$a^t\equiv 1(\bmod m)$，其中$t=\phi(m)$．也可不用那个定理将这一点证明如下．若$(a,\ m)=1$，则$a,\ a^2,\ a^3,\ \cdots$的最小剩余$(\bmod m)$都与m互素．与m互素的最小剩余$(\bmod m)$有$\phi(m)$个，而a的乘幂却有无限多个，故必有正整数j和k，$j\neq k$，使$a^j\equiv a^k(\bmod m)$．因$(a,\ m)=1$，上述同余式中a的较小次幂可以约去，我们有

$$a^{j-k}\equiv 1(\bmod m) \quad 或 \quad a^{k-j}\equiv 1(\bmod m).$$

因此，若$(a,\ m)=1$，则存在着正整数t使$a^t\equiv 1(\bmod m)$．事实上，这样的数有着无限多个，这是因为，当$(a,\ m)=1$时，$a^{\phi(m)}\equiv 1(\bmod m)$，而对任何正整数$k$，都有

$$a^{t+k\phi(m)}\equiv a^t(a^k)^{\phi(m)}\equiv a^t\equiv 1(\bmod m).$$

这种正整数中最小的一个称为a对模m的阶．例如，对模7，我们有

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1.

故对模7，3和5的阶为6，2和4的阶为3，6的阶为2，1的

阶为1. 当高斯引进这一概念时，他把 t 称为 a 所属的指数 $(\bmod m)$. 高斯所用的术语比我们的称呼要长，但却更为常用.

【练习1】 3, 5, 7对模8的阶各是多少?

一个整数的阶$(\bmod m)$并非可以为任何数，下面我们就要说明，它一定是 $\phi(m)$ 的一个因子.

引理1 若 $(a, m)=1$, $a^n\equiv1(\bmod m)$, $n>0$, 且 a 的阶 $(\bmod m)$ 为 t, 则 $t|n$.

证明 假设 $(t, n)=d$, 则我们知存在整数 r 和 s 使

$$rt+sn=d.$$

因而
$$a^d=a^{rt+sm}=(a^t)^r(a^n)^s.$$

但根据假定，$a^n\equiv a^t\equiv1(\bmod m)$, 故 $a^d\equiv1(\bmod m)$. 而 t 已被假定是满足 $a^t\equiv1(\bmod m)$ 的最小正整数，故 $t\leqslant d$. 又因 $(t, n)=d$, 故 d 是 t 的一个因子，所以 $d\leqslant t$. 于是，$d=t$. 由此即知，t 是 n 的一个因子. 上述证明中，我们忽略了 r 和 s 中有一个为负数的情况，其补救办法是，用 $a^n(a^{-n})\equiv1(\bmod m)$ 来定义 $n>0$ 时的 $a^{-n}(\bmod m)$.

定理1 若 $(a, m)=1$, a 的阶 $(\bmod m)$ 为 t, 则 $t|\phi(m)$.

证明 由欧拉对费马定理的推广(上节定理1)知，

$$a^{\phi(m)}\equiv1(\bmod m).$$

在引理1中令 $n=\phi(m)$, 即可得结果.

【练习2】 一个整数的阶可为哪些数? 各举一例.

我们证明下列定理，它也是应用上述想法的一个例子.

定理2 若 p 和 q 为奇素数，且 $q|(a^p-1)$, 则或有 $q|(a-1)$, 或有 $q=2kp+1$, 其中 k 某整数.

证明 因 $q|(a^p-1)$, 我们有 $a^p\equiv1(\bmod q)$. 故由引理1, a 的阶 $(\bmod q)$ 是 p 的一个因子，即 a 的阶为1或 p. 若 a 的

阶为1，即$a^1\equiv 1 \pmod q$，故$q|(a-1)$．另一方面，若a的阶为p，则由定理1，$p|\phi(q)$，或$p|(q-1)$．即对某整数r，有$q-1=rp$．又由于p和q是奇数，r就一定是偶数，定理得证．

推论 2^p-1的任何因子必取$2kp+1$的形式．

【练习3】 根据这一推论，$2^{19}-1$的最小素因子是什么数？

如a的阶$(\bmod m)$为$\phi(m)$，我们把a称为m的一个**原根**．

原根以及具有原根的数之所以特别重要，是由于下列性质所致：

定理3 若g是m的一个原根，则

$$g,\ g^2,\ \cdots,\ g^{\phi(m)}$$

各数对模m的最小剩余，恰是小于m且与m互素的$\phi(m)$个正整数的一个排列．

例如，2是9的一个原根，而它的各次乘幂为

$$2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6;$$

它们的最小剩余$(\bmod 9)$分别为

$$2,\ 4,\ 8,\ 7,\ 5,\ 1.$$

定理3的证明 因$(g,\ m)=1$，g的各次幂都与m互素．另外，若

$$g^j\equiv g^k \pmod m,\ 1\leqslant j\leqslant \phi(m),\ 1\leqslant k\leqslant \phi(m),$$

且假定$j\geqslant k$（这样做并不失一般性），则

$$g^{j-k}\equiv 1 \pmod m.$$

但$0\leqslant j-k<\phi(m)$；且因g是m的一个原根，故仅当$t=0$时才能有

$$g^t\equiv 1 \pmod m,\ 0\leqslant t<\phi(m).$$

因此$j-k=0$，或$j=k$．

【练习 4】 证明：3 是 7 的一个原根.

【练习 5】 用尝试法求 10 的一个原根.

并不是每个整数都有原根．例如，我们在练习 1 中已经看到，8 就没有原根．现在我们要着手证明，每个素数都有原根．其证明不大容易，要作许多准备工作(引理 2 到引理 4)；同时，由于这是一个存在性证明，它并未说明如何将原根求出来．鉴于这些原因，要是你直接相信这一结论，也未必会失去多少东西；放心好了，这个结论是正确的.

如 a 的阶 $(\mathrm{mod}\, p)$ 为 d，则对于 $k=1, 2, \cdots, d$，有

$$(a^k)^d \equiv 1 \pmod p.$$

于是，在整数 $a^2, a^3, \cdots, a^d$ 中，有些数的阶是 d，有些数的阶则要小一些，例如 a^d 的阶就是 1.

【练习 6】 3 的阶 $(\mathrm{mod}\, 10)$ 为 4，求 $3^2, 3^3, 3^4$ 的阶 $(\mathrm{mod}\, 10)$

下一引理指出了 a 的哪些乘幂与 a 的阶相同.

引理 2 假设 a 的阶 $(\mathrm{mod}\, p)$ 为 d，那么，当且仅当 $(k, d)=1$ 时，a^k 的阶 $(\mathrm{mod}\, p)$ 也为 d.

证明 设 $(k, d)=1$，并记 a^k 的阶为 t．我们有

$$1 \equiv (a^d)^k \equiv (a^k)^d \pmod p,$$

故由引理 1 知，$t \mid d$．又由于 t 是 a^k 的阶，

$$(a^k)^t \equiv a^{kt} \equiv 1 \pmod p,$$

故同样由引理 1，$d \mid kt$．因 $(k, d)=1$，故 $d \mid t$．再加上 $t \mid d$，就有 $t=d$.

为了证明其逆，假定 a 和 a^k 的阶都是 d，且 $(k, d)=r$．于是有

$$1 \equiv a^d \equiv (a^d)^{k/r} = (a^k)^{d/r} \pmod p.$$

因为 d 是 a^k 的阶，引理 1 表明，$d \mid d/r$，这就意味着 $r=1$.

现在我们需要一个关于多项式同余式的解的引理．虽然

这是一个重要的结论，但我们在其它地方却用不到它.

引理 3 若 f 是 n 次多项式，则

(1) $$f(x)\equiv 0 \pmod p$$

至多有 n 个解.

证明 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

它的次数为 n，即 $a_n\not\equiv 0 \pmod p$. 我们用归纳法证明这一引理. 对于 $n=1$，因为 $(a_1, p)=1$，故

$$a_1x+a_0\equiv 0 \pmod p$$

只有一解. 假定引理对 $n-1$ 次多项式成立. 设 f 的次数为 n. $f(x)\equiv 0$ 要末无解，要末至少有一解. 在第一种情况下，引理已经得证. 在第二种情况下，可假定 r 就是一解，即

$$f(r)\equiv 0 \pmod p,$$

且 r 是一个最小剩余 $\pmod p$. 那么，由于 $t=0, 1, \cdots, n$ 时，$x-r$ 都是 x^t-r^t 的一个因子，我们有

$$\begin{aligned} f(x)&\equiv f(x)-f(r)\\ &\equiv a_n(x^n-r^n)+a_{n-1}(x^{n-1}-r^{n-1})+\cdots+a_1(x-r)\\ &\equiv (x-r)g(x) \pmod p, \end{aligned}$$

其中 $g(x)$ 是一个 $n-1$ 次多项式. 假定 s 也是 (1) 的一个解，因此，

$$f(s)\equiv (s-r)g(s)\equiv 0 \pmod p.$$

由于 p 是素数，故

$$s\equiv r \pmod p \quad 或 \quad g(s)\equiv 0 \pmod p.$$

由归纳法假定，第二个同余式至多有 $n-1$ 个解. 而第一个同余式只有一解，因而引理得证.

注意，若模不是素数，引理 3 未必成立. 例如，

$$x^2+x\equiv 0 \pmod 6$$

有 4 个解：0, 2, 3, 5.

引理 4 若 $d\mid(p-1)$，则 $x^d\equiv 1 \pmod p$ 恰有 d 个解.

证明 由费马定理，同余式 $x^{p-1}\equiv 1 \pmod p$ 恰有 $p-1$ 个解，它们是 $1, 2, \cdots, p-1$. 此外，

$$\begin{aligned} x^{p-1}-1 &= (x^d-1)(x^{p-1-d}+x^{p-1-2d}+\cdots+1) \\ &= (x^d-1)h(x). \end{aligned}$$

由引理 3，我们知 $h(x)\equiv 0 \pmod p$ 至多有 $p-1-d$ 个解. 因此 $x^d\equiv 1 \pmod p$ 至少有 d 个解. 再用引理 3，我们知它正好有 d 个解.

我们终于作好了准备，以证明下列定理：

定理 4 每一素数 p 具有 $\phi(p-1)$ 个原根.

证明 定理 1 说明

$$1,\ 2,\ \cdots,\ p-1 \tag{2}$$

中，每个整数的阶都是 $p-1$ 的一个因子. 对于 $p-1$ 的每一因子 d，用 $\psi(d)$ 记 (2) 中其阶为 d 的整数的个数，我们刚说过的结论可改述为

$$\sum_{d\mid(p-1)}\psi(d)=p-1.$$

由 § 9 定理 4，我们有

$$\sum_{d\mid(p-1)}\psi(d)=\sum_{d\mid(p-1)}\phi(d). \tag{3}$$

如果我们能证，对每个 d 有 $\psi(d)\leqslant\phi(d)$，由 (3) 即可得，对每个 d 有 $\psi(d)=\phi(d)$. 特别地，p 的原根数就是

$$\psi(p-1)=\phi(p-1).$$

选取某个 d. 如果 $\psi(d)=0$，于是 $\psi(d)<\phi(d)$，结论就已证得. 如果 $\psi(d)\neq 0$，于是存在一个阶为 d 的整数，称作 a. 根据引理 4，同余式

$$x^d\equiv 1 \pmod p \tag{4}$$

恰有 d 个解，并且下列 d 个整数满足 (4)：

(5) $$a,\ a^2,\ a^3,\ \cdots,\ a^d.$$

又因这些整数中任意两数的最小剩余(mod p)均不相同，所以它们就是(4)的所有解. 由引理 2, (5)中阶为 d 的数就是那些满足 $(k, d)=1$ 的乘幂 a^k. 但这种 k 一共有 $\phi(d)$ 个，故在这一情况下有 $\psi(d)=\phi(d)$. 前面已经提到，定理的证明即可结束.

我们实际上证得了比定理 4 所述还要更多的结论. 尽管以后并不要用上面附带证得的结论，但仍有必要将它叙述成以下推论.

推论 若 p 为素数，$d|(p-1)$，则阶为 d 的最小剩余(mod p)的个数为 $\phi(d)$.

【练习 7】 利用本节开头的乘幂表(mod 7)，验证 $p=7$ 时上述推论成立.

定理 4 实际上并没有帮助我们求出一个素数的原根. 为了求出一个原根，我们可以使用表格或者进行尝试. 下表列出了 100 以内各个素数 p 的最小正原根 g_p:

p	2	3	5	7	11	13	17	19	23	29	31	37	41
g_p	1	2	2	3	2	2	3	2	5	2	3	2	6
p	43	47	53	59	61	67	71	73	79	83	89	97	
g_p	3	5	2	2	2	2	7	5	3	2	3	5	

还没有找到一个方法能预测一个给定素数 p 的最小正原根是什么数，关于 $\phi(p-1)$ 个原根在对模 p 的最小剩余中的分布情况知道得也不多. 例如，71 和 73 的原根为

71 的原根						73 的原根					
7	11	13	21	22	28	5	11	13	14	15	20
31	33	35	42	44	47	26	28	29	31	33	34
52	53	55	56	59	61	39	40	42	44	45	47
62	63	65	67	68	69	53	58	59	60	62	68

除了素数以外，还有其它数也存在原根. 可以证明，具有原根的所有正整数为 1, 2, 4, p^e 和 $2p^e$，其中 p 是奇素数，e 是正整数.

【练习 8】 整数 2, 3, …, 25 中，哪些没有原根？

作为应用原根的例子，我们将使用原根迅速而巧妙地证明威尔逊定理的一部分. 设 g 是奇素数 p 的一个原根. 由定理 3, 我们知 g, g^2, …, g^{p-1} 的最小剩余 $(\bmod p)$ 是 1, 2, …, $p-1$ 的一个排列. 将它们相乘，并利用下式(参见附录一)：

$$1+2+3+\cdots+(p-1)=(p-1)p/2,$$

我们得 $$1\cdot 2\cdot\cdots\cdot(p-1)\equiv g\cdot g^2\cdot\cdots\cdot g^{p-1}(\bmod p),$$

或 $$(p-1)!\equiv(g^p)^{(p-1)/2}\equiv g^{(p-1)/2}(\bmod p).$$

但 $g^{(p-1)/2}$ 满足 $x^2\equiv 1(\bmod p)$，而由 § 6 引理 2 或本节引理 4, 我们知

$$g^{(p-1)/2}\equiv 1 \quad 或 \quad -1(\bmod p).$$

但是，第一种情况是不可能的，因为 g 是 p 的一个原根. 因此，$(p-1)!=-1(\bmod p)$.

对数的概念无疑是很有用的，如果 m 是具有原根的整数，那么类似的概念也可以给对模 m 的整数作出定义. 设 g 是 m 的一个原根，对于满足 $(k, m)=1$ 的 k, k 关于 g 的指数 $(\bmod m)$ 定义为一整数 t，使

(6) $$g^t\equiv k(\bmod m).$$

由于 m 具有原根，这样的 t 是存在的. k 关于 g 的最小指数 $(\bmod m)$ (记为 $\mathrm{ind}_g k$)是指整数 t，它不但满足(6)，而且是一个最小剩余 $(\bmod \phi(m))$. 这样的数是存在的，因为由(6)可知，要是 t_1 和 t_2 都是 k 的指数 $(\bmod m)$，则 $t_1\equiv t_2(\bmod \phi(m))$. 例如，考虑 5 的原根 2, 我们有

$$2^0\equiv 1,\ 2^1\equiv 2,\ 2^2\equiv 4,\ 2^3\equiv 3(\bmod 5),$$

故 $\mathrm{ind}_2 1=0,\ \mathrm{ind}_2 2=1,\ \mathrm{ind}_2 4=2,\ \mathrm{ind}_2 3=3.$

【练习 9】 计算各个整数关于原根5的最小指数(mod 7).

指数与对数一样,在计算中是很有用的.

定理 5 若m是具有原根的一数, $\mathrm{ind}_g k$ 表示 k 关于原根 g 的最小指数(mod m),则

(7) $$\mathrm{ind}_g ab\equiv \mathrm{ind}_g a+\mathrm{ind}_g b \pmod{\phi(m)},$$

(8) $$\mathrm{ind}_g a^n\equiv n\cdot \mathrm{ind}_g a \pmod{\phi(m)}.$$

证明 设 $\mathrm{ind}_g a=r$, $\mathrm{ind}_g b=s$, 则 $g^r\equiv a$, $g^s\equiv b \pmod m$. 于是

$$ab\equiv g^{r+s} \pmod m.$$

因此,$r+s$ 是 ab 的一个指数(mod m). 故

$$\mathrm{ind}_g ab\equiv r+s \pmod{\phi(m)}.$$

(7)式得到了证明. 反复应用(7)可证得(8)式.

【练习 10】 验证,对模 7, 成立

$$\mathrm{ind}_5 2+\mathrm{ind}_5 6\equiv \mathrm{ind}_5 12,$$

$$6\,\mathrm{ind}_5 2\equiv \mathrm{ind}_5 64.$$

和对数一样, 指数使乘法问题转化为加法问题. 若有一张关于m的任一原根的最小指数表(mod m), 那么利用定理5, 我们就能较容易地求解同余式, 正如关于任意底数的对数表能简化实数的计算一样. 例如, 利用 19 的原根 2, 我们可以作出如下最小指数表:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2 n$	0	1	13	2	16	14	6	3	8	17	12	15
n	13	14	15	16	17	18						
$\mathrm{ind}_2 n$	5	7	11	4	10	9.						

这样一张表可以用来求解同余式. 例如,若

$$13x\equiv 16 \pmod{19},$$

那么，由定理 5,

$$\mathrm{ind}_2 13x \equiv \mathrm{ind}_2 13 + \mathrm{ind}_2 x \equiv \mathrm{ind}_2 16 \pmod{18};$$

利用上表，得

$$\mathrm{ind}_2 x \equiv 4-5 \equiv 17 \pmod{18}.$$

再由上表得知 $x \equiv 10 \pmod{19}$. 又如

$$x^{13} \equiv 16 \pmod{19},$$

用其它方法求解就很困难，而由定理 5,

$$13\,\mathrm{ind}_2 x \equiv \mathrm{ind}_2 16 \equiv 4 \pmod{18},$$

由此解得 $\mathrm{ind}_2 x \equiv 10 \pmod{18}$. 故由上表知，$x \equiv 17 \pmod{19}$ 就是原同余式的解.

习　　题

1. 下列整数中，哪些具有原根？
   (a) 198, 199, 200, 201, 202, 203;
   (b) 10198, 10199, 10200, 10201, 10202, 10203.
2. 2, 4, 7, 8, 11, 13, 14 对模 15 的阶分别是多少？
3. (a) 作出关于原根 2 的最小指数表 $(\mathrm{mod}\ 29)$;
   (b) 利用此表求解 $9x \equiv 2 \pmod{29}$;
   (c) 利用此表求解 $x^9 \equiv 2 \pmod{29}$.
4. 已知 $\mathrm{ind}_5 45 \equiv 45 \pmod{96}$，下列同余式各有多少解？
   (a) $x^7 \equiv 45 \pmod{97}$;　　(b) $x^8 \equiv 45 \pmod{97}$;
   (c) $x^9 \equiv 45 \pmod{97}$.
5. (a) 证明 2 是 19 的一个原根；
   (b) 证明 2 不是 23 的一个原根；
   (c) 10 是 11 的一个原根吗？
6. 若 $(a, m) \neq 1$，是否存在 t 使 $a^t \equiv 1 \pmod{m}$？
7. 甲说："看！这五页计算表明：$457^{911} \equiv 1 \pmod{10021}$."乙看了一下表 C 和表 A 后，说："你错了."乙对不对？
8. 若 g 是 m 的一个原根，证明：当且仅当 $a \equiv b \pmod{\phi(m)}$ 时，有 $g^a \equiv g^b \pmod{m}$.

9. (a) 证明：若 g 是 p 的一个原根，则当 $(k, p-1)=1$ 时，g^k 的最小剩余也是 p 的原根；

(b) 求 37 的 12 个原根.

10. (a) 求 11 的所有原根；

(b) 7 关于上述每个原根的指数是什么?

11. 若 g 是素数 p 的一个原根，证明 $\mathrm{ind}_g(-1)=(p-1)/2$.

12. 假定 2 是奇素数 p 的一个原根，且 $\mathrm{ind}_2(p-1)=r$.

(a) 证明 $\mathrm{ind}_2(p-2)=r+1$;

(b) 若 $\mathrm{ind}_2 x=r+2$, x 是什么数?

13. 哪些整数对模 31 的阶为 6?

14. 若 a 对模 p 的阶为 e，证明

$$a^{e-1}+a^{e-2}+\cdots+1\equiv 0 \pmod p.$$

15. (a) 若 g 和 h 是奇素数 p 的原根，则对某整数 a，有 $g\equiv h^a \pmod p$，证明 a 为奇数；

(b) 证明：若 g 和 h 为奇素数 p 的原根，则 gh 的最小剩余不是 p 的一个原根.

16. 证明：若 a 的阶 $(\mathrm{mod}\, p)$ 为 3，则 $a+1$ 的阶 $(\mathrm{mod}\, p)$ 为 6.

17. 证明 $131{,}071=2^{17}-1$ 为素数.

18. 证明：若 p 和 q 为奇素数，$q\mid(a^p+1)$，则或有 $q\mid(a+1)$，或有 $q=2kp+1$，其中 k 为某整数.

19. 证明：$(2^{19}+1)/3$ 为素数.

20. 若 g 是素数 p 的一个原根，证明：对任一 n，$\mathrm{ind}_g(n-1)$，$\mathrm{ind}_g n$ 和 $\mathrm{ind}_g(n+1)$ 都不能构成算术级数.

21. (a) 证明：若 m 是具有原根的一数，则小于或等于 m 且与 m 互素的正整数之积与 -1 同余 $(\mathrm{mod}\, m)$；

(b) 证明：若 m 没有原根，(a) 中结论未必总能成立.

22. 大家知道，$(\log_a b)(\log_b a)=1$.

(a) 关于指数的类似结论是什么?

(b) 证明这一结论.

23. 若 $\log_a b=\log_b a$，则我们知道 $b=a$ 或 $b=1/a$. 假定 g 和 h 是一个奇素数 p 的原根，且 $\mathrm{ind}_g h=\mathrm{ind}_h g$，我们可以得出什么结论?

§11 二次同余式

研究了线性同余式以后，很自然地要观察一下二次同余式：

$$Ax^2+Bx+C\equiv 0 \pmod m.$$

在本节中，我们将限于模为奇素数的情况；在附录三中，我们会看到怎样处理一般的二次同余式.

我们将假定 $A\not\equiv 0 \pmod p$，因为若 $A\equiv 0 \pmod p$，则

(1) $$Ax^2+Bx+C\equiv 0 \pmod p$$

不再是二次同余式，而是线性同余式了. 我们还知道，存在着整数 A'，使 $AA'\equiv 1 \pmod p$，因此(1)与下式具有相同的解：

(2) $$x^2+A'Bx+A'C\equiv 0 \pmod p.$$

【练习 1】 将 $2x^2+3x+1\equiv 0 \pmod 5$ 化为首项系数为 1 的二次同余式.

若 $A'B$ 为偶数，我们可在(2)中配方，得

$$\left(x+\frac{A'B}{2}\right)^2\equiv\left(\frac{A'B}{2}\right)^2-A'C \pmod p;$$

若 $A'B$ 为奇数，我们可将它变为 $p+A'B$，它是偶数，然后再配方. 所以，无论在哪种情况下，我们都用了一个与 (1) 等价且有下列形式的同余式来代替(1)：

(3) $$y^2\equiv a \pmod p.$$

因此，如我们能解这种同余式，我们就能求解任何二次同余式 $\pmod p$.

【练习 2】 将练习 1 中的同余式化为形式(3).

【练习 3】(选做) 用观察法求出练习 2 中同余式的所有解.

这种同余式并非都有解. 例如, 对模 5,

$$0^2\equiv 0,\ 1^2\equiv 4^2\equiv 1,\ 2^2\equiv 3^2\equiv 4.$$

故 $x^2\equiv a \pmod 5$ 对 $a=0, 1, 4$ 有解, 但对 $a=2, 3$ 却无解. 我们还注意到, $x^2\equiv 0 \pmod p$ 只有一解 $x\equiv 0 \pmod p$. 现在我们来证, 若 $p\nmid a$, 则 $x^2\equiv a \pmod p$ 的解必成对出现. 这也并不奇怪, 由于 $r^2=(-r)^2$, 我们有 $r^2\equiv(-r)^2 \pmod p$, 故若 r 为 $x^2\equiv a \pmod p$ 的解, 则 $-r$ 的最小剩余 $(\bmod p)$ 也是它的解. 因此, 若 r 是一解, 则 $p-r$ 也是一解.

定理 1 假定 p 为奇素数, 若 $p\nmid a$, 则 $x^2\equiv a \pmod p$ 恰有两解或无解.

证明 假定此同余式有一个解, 称为 r, 则 $p-r$ 也为一解, 且它不同于 r. (因为若 $r\equiv p-r \pmod p$, 则 $2r\equiv 0 \pmod p$; 由于 $(2, p)=1$, 我们得 $r\equiv 0 \pmod p$, 但这是不可能的.) 又若 s 为任一解, 则 $r^2\equiv s^2 \pmod p$, 因此, $p\mid(r-s)(r+s)$. 于是,

$$p\mid(r-s)\ \text{或}\ p\mid(r+s).$$

在第一种情况下, $s\equiv r \pmod p$; 在第二种情况下, $s\equiv p-r \pmod p$. 由于 s, r 和 $p-r$ 全为最小剩余, 我们有 $s=r$ 或 $s=p-r$, 因此, r 和 $p-r$ 就是仅有的解.

若模不是素数, 这一定理未必成立. 例如, $x^2\equiv 1 \pmod 8$ 有 4 个解.

【练习 4】 若 $p>3$, $x^2\equiv 4 \pmod p$ 的两个解是什么?

由定理 1 可得, 若 a 在整数 $1, 2, \cdots, p-1$ 中挑选, 则 $x^2\equiv a \pmod p$ 对于 a 的 $(p-1)/2$ 个值有两解, 对于 a 的其余 $(p-1)/2$ 个值无解. 例如, $x^2\equiv a \pmod 7$ 对 $a=1, 2, 4$ 有两

解，对 $a=3, 5, 6$ 无解，这从下表也可看出：

x	1	2	3	4	5	6
$x^2 (\bmod 7)$	1	4	2	2	4	1.

【练习 5】 对于 a 的哪些值，$x^2 \equiv a(\bmod 11)$ 有两解？

要是能将这两组值区分开来就好了. 为了做到这一点，我们将在本节中推导欧拉准则：

定理 2 若 p 为奇素数，且 $p \nmid a$，则 $x^2 \equiv a(\bmod p)$ 有解或无解取决于

$$a^{(p-1)/2} \equiv 1 \text{ 或 } -1(\bmod p).$$

首先，我们引进几个新名称：若 $x^2 \equiv a(\bmod m)$ 有解，则 a 称为一个二次剩余 $(\bmod m)$；若此同余式无解，则 a 称为一个二次非剩余 $(\bmod m)$. 还有三次剩余、四次剩余等等. 在不致发生混淆时，我们将把"二次"这一形容词省去，简短地称"剩余"或"非剩余".

欧拉准则利用原根容易推得.

定理 2 的证明 设 g 为奇素数 p 的一个原根，则对某 k，有 $a \equiv g^k (\bmod p)$. 若 k 为偶数，则 $x^2 \equiv a(\bmod p)$ 便有一解，即为 $g^{k/2}$ 的最小剩余；又由费马定理，

$$a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} \equiv (g^{k/2})^{(p-1)} \equiv 1(\bmod p).$$

若 k 为奇数，则

$$a^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k \equiv -1(\bmod p),$$

$x^2 \equiv a(\bmod p)$ 就没有解，因为若它有一解，比方说 r，我们会有

$$1 \equiv r^{p-1} \equiv (r^2)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv -1(\bmod p),$$

这是不可能的.

作为应用这个准则的一例，让我们看一看 $x^2 \equiv 7(\bmod 31)$ 是否有解. 我们应算出 $7^{(31-1)/2} = 7^{15}$，并看看它除以 31 所得

之余数．当然，我们不必实际地去做此除法：我们有

$$7^2 \equiv 49 \equiv 18 \pmod{31},$$

两边平方，我们得

$$7^4 \equiv 18^2 \equiv 324 \equiv 14 \pmod{31},$$

$$7^8 \equiv 14^2 \equiv 196 \equiv 10 \pmod{31},$$

以及
$$7^{16} \equiv 10^2 \equiv 100 \equiv 7 \pmod{31}.$$

因 7 与 31 互素，我们可用 7 除最后一个同余式而得 $7^{15} \equiv 1 \pmod{31}$．因此根据欧拉准则可得 $x^2 \equiv 7 \pmod{31}$ 有解．

虽然欧拉准则能告诉我们 $x^2 \equiv a \pmod{p}$ 何时有解，但它并未给出实际求解的方法．当然，可以令 $x=1, 2, 3, 4, \cdots$，逐一依次代入，直到求得解为止，但这一做法冗长繁琐．有时，下列方法比较方便：在同余式右边加上模的倍数，并将平方因子析出．例如，取 $x^2 \equiv 7 \pmod{31}$，我们已经知道它是有解的，重复地加上 31，我们有

$$x^2 \equiv 7 \equiv 38 \equiv 69 \equiv 100 \equiv 10^2 \pmod{31},$$

我们立即可知，当 $x=10$ 或 -10 时，同余式得到满足，故 10 和 21 就是它的两个解．此例比较容易，一个更典型的例子是：$x^2 \equiv 41 \pmod{61}$．使用欧拉准则知有解存在．我们有

$$x^2 \equiv 41 \equiv 102 \equiv 163 \equiv 224 \equiv 4^2 \cdot 14 \pmod{61}.$$

故
$$(x/4)^2 \equiv 14 \equiv 75 \equiv 5^2 \cdot 3 \pmod{61}.$$

因此，
$$(x/4 \cdot 5)^2 \equiv 3 \equiv 64 \equiv 8^2 \pmod{61},$$

以及
$$x^2 \equiv (4 \cdot 5 \cdot 8)^2 \equiv 160 \equiv 38^2 \pmod{61}.$$

因此，$x \equiv \pm 38 \pmod{61}$，从而两个解为 38 和 23．使用这一方法，经过或多或少的计算，总能求出其解．

【练习 6】　求 $x^2 \equiv 8 \pmod{31}$ 之解．

欧拉准则用起来有时非常麻烦，甚至对于数字较小的一些同余式，如 $x^2 \equiv 320 \pmod{8191}$，也是如此．现在我们提出

一种方法，它能决定一个整数何时为二次剩余(mod p)．这一方法用起来比较容易，即使有关的数是3201和8191时，也是如此．该方法的基础是有名的二次互反性定理，这一定理我们将要用到，而且它还有许多其它的应用．

首先我们介绍一种记号，以简化"$x^2\equiv a \pmod p$有解"这一较长的说法．我们定义勒让德(Legendre)记号(a/p)如下：设p为奇素数，且$p\nmid a$，则

$$(a/p)=\begin{cases}1, & \text{当 } a \text{ 是二次剩余}\pmod p\text{时；}\\ -1, & \text{当 } a \text{ 是二次非剩余}\pmod p\text{时．}\end{cases}$$

例如，$(3/5)=-1$，因为$x^2\equiv 3 \pmod 5$无解；$(1/5)=1$，因为1是二次剩余(mod 5)．$(7/15)$和$(91/7)$则都没有意义，这是因为，在第一个记号中，15不是奇素数，在第二个记号中，$7|91$．

【练习7】 $(1/3)$，$(1/7)$，$(1/11)$ 各是什么？一般地，$(1/p)$是什么？

【练习8】 $(4/5)$是什么？$(4/7)$是什么？当p为任一奇素数时，$(4/p)$是什么？

【练习9】(选做) 由前两个练习推出一个定理．

要知道$x^2\equiv 3201 \pmod{8191}$是否有解，我们可计算$(3201/8191)$．为此，我们需要一些如何运用勒让德记号的规则．我们先介绍三条简单而重要的性质．

定理3 勒让德记号具有下列性质：

(A) 若$a\equiv b \pmod p$，则$(a/p)=(b/p)$；

(B) 若$p\nmid a$，则$(a^2/p)=1$；

(C) 若$p\nmid a$，$p\nmid b$，则$(ab/p)=(a/p)(b/p)$．

在上述性质以及本节的以下全部内容中，我们约定，p和q代表奇素数，而且勒让德记号中的第一个数都不是第二个数的倍数．有了这些规定，所有勒让德记号就都有确定的意

义了.

定理3的证明 (A): 设 $x^2\equiv a(\bmod p)$ 有解. 若 $a\equiv b(\bmod p)$, 则 $x^2\equiv b(\bmod p)$有解, 且解相同. 这就说明了

(4) 若 $(a/p)=1,\ a\equiv b(\bmod p)$, 则 $(b/p)=1$.

【练习 10】 验证下列结论:

(5) 若 $(a/p)=-1,\ a\equiv b(\bmod p)$, 则 $(b/p)=-1$.

(4)和(5)合在一起, 就说明了(A)是正确的.

(B): 显然, $x^2\equiv a^2(\bmod p)$ 具有一解, 它就是 a 的最小剩余$(\bmod p)$.

(C): 勒让德记号这一性质, 再加上二次互反性定理, 使得这种记号在计算中非常有用. 性质(C)用普通语言说起来就是: 两个剩余的乘积是一剩余, 两个非剩余的乘积也是一剩余, 一个剩余和一个非剩余的乘积是一非剩余. 为了证明(C), 我们要用欧拉准则: 用勒让德记号来说, 它就是

$$(a/p)=\begin{cases}1, & 若\ a^{(p-1)/2}\equiv 1(\bmod p),\\ -1, & 若\ a^{(p-1)/2}\equiv -1(\bmod p).\end{cases}$$

比较一下"1"和"−1"出现的情况, 我们看到

(6) $$(a/p)\equiv a^{(p-1)/2}(\bmod p).$$

所以, 由(6)以及$(xy)^n\equiv x^ny^n(\bmod p)$, 我们有

$$\begin{aligned}(ab/p)&\equiv(ab)^{(p-1)/2}\equiv a^{(p-1)/2}b^{(p-1)/2}\\ &\equiv(a/p)(b/p)(\bmod p).\end{aligned}$$

(C)我们还未证完, 我们只证明了

$$(ab/p)\equiv(a/p)(b/p)(\bmod p).$$

但此同余式左端只能是1或−1, 右端也一样, 这两数对模 p 要同余, 只有它们相等才行, 我们就证得了(C).

我们也可用(6)来简捷地证明(A)与(B). 例如, 要证明(B), 由(6)和费马定理, 我们有

$$(a^2/p)\equiv(a^2)^{(p-1)/2}\equiv a^{p-1}\equiv 1 \pmod p.$$

由于(a^2/p)只能是 1 或 -1，故由上式得$(a^2/p)=1$.

【练习 11】 借助于(6)证明(A).

【练习 12】 证明：对一切 a 和 p，有$(4a/p)=(a/p)$.

【练习 13】 利用(A)和(B)计算$(19/5)$和$(-9/13)$.

二次互反性定理将告诉我们(p/q)和(q/p)间有什么关系. 在它首次为高斯(Gauss)证明以前很久，欧拉就已经猜到了它，后来高斯又给出了好几种证法. 一些深刻而又重要的结论是通过观察而得出的，二次互反性定理即为一例. 考虑以下两张表：

q \ p	5	7	11	13	17	19	23
3	-1	1	-1	1	-1	1	-1
5		-1	1	-1	-1	1	-1
7			1	-1	-1	-1	1
11				-1	-1	-1	-1
13					1	-1	1
17						1	-1
19							1

(p/q)

q \ p	5	7	11	13	17	19	23
3	-1	-1	1	1	-1	-1	1
5		-1	1	-1	-1	1	-1
7			-1	-1	-1	1	-1
11				-1	-1	1	1
13					1	-1	1
17						1	-1
19							-1

(q/p)

根据观察你能看出(p/q)与(q/p)间的关系吗？要有把握地作出任何猜想，这两张表也许太小了．不过，仍可注意到，两表中，相应于$p=5$, 13, 17 的各列是分别相同的，相应于这三个数的各行也分别相同．5, 13, 17 这三个数的性质是，它们都与 1 同余 (mod 4)，29 以内的其它素数却没有这一性质．根据这一点，我们可以作出下列正确的猜测：

若p和q中有一数与 1 同余(mod 4)，则$(p/q)=(q/p)$．表中不合这一规则的那些数从一表跑到另一表时，要改变符号，这一情况可用下列假设来解释：

若p和q均与 3 同余 (mod 4)，则$(p/q)=-(q/p)$．事实上，上述两个猜测是普遍成立的，它们构成了如下定理．

定理 4 (二次互反性定理)　设p和q为奇素数，若$p\equiv q\equiv 3 \pmod 4$，则$(p/q)=-(q/p)$，否则，有$(p/q)=(q/p)$．

我们将这一定理放到下节去证明，但是，尽管未证，我们仍将毫不犹豫地应用这一定理．假定我们要知道$x^2\equiv 85 \pmod{97}$是否有解，也就是要计算$(85/97)$．用定理 3 和定理 4，我们就能将计算进行到底．根据定理 3 性质 (C)，我们有

$$(85/97)=(17\cdot 5/97)=(17/97)(5/97). \tag{7}$$

我们将 (7) 中两个因子分开进行计算．因$97\equiv 1 \pmod 4$(还有$17\equiv 1 \pmod 4$)，二次互反性定理说明，

$$(17/97)=(97/17).$$

定理 3 性质(A)说明，

$$(97/17)=(12/17).$$

而

$$\begin{aligned}(12/17)&=(4\cdot 3/17)=(4/17)(3/17) && (\text{根据(C)})\\ &=(3/17) && (\text{根据(B)})\\ &=(17/3) && (\text{根据定理 4})\end{aligned}$$

$$=(2/3) \qquad \text{(根据 (A))}$$
$$=-1. \qquad \text{(根据观察)}$$

另一个因子要简单些:

$$(5/97)=(97/5) \qquad \text{(根据定理 4)}$$
$$=(2/5) \qquad \text{(根据 (A))}$$
$$=-1. \qquad \text{(根据观察)}$$

将这些计算结果代回(7),我们得

$$(85/97)=(17/97)(5/97)=(-1)(-1)=1;$$

因此,原同余式有解.若先利用性质(A),我们也可通过另一途径算出(85/97):

$$(85/97)=(-12/97)=(-1/97)(4/97)(3/97)$$
$$=(-1/97)(3/97).$$

我们知 $(3/97)=(97/3)=(1/3)=1$,

故 $(85/97)=(-1/97)$;如果我们知道了 $(-1/97)$,也就能得知 $(85/97)$.

如果你考察了关于勒让德记号的许多例子,就会明白,为了应用定理 3 和定理 4 来计算任一勒让德记号的值,只要知道 $(-1/p)$ 和 $(2/p)$ 对于任意 p 其值是什么就够了.根据欧拉准则,我们能很快地求得 $(-1/p)$:

定理 5 若 p 为奇素数,则

$$(-1/p)=\begin{cases}1, & \text{若 } p\equiv 1 \pmod 4, \\ -1, & \text{若 } p\equiv 3 \pmod 4.\end{cases}$$

换言之,-1 是与 1 同余(mod 4)的素数的二次剩余,并是其它奇素数的二次非剩余.

证明 欧拉准则称,

$$(-1/p)\equiv(-1)^{(p-1)/2} \pmod p,$$

由于 $(p-1)/2$ 是偶数还是奇数取决于 p 与 1 同余还是与 3

同余(mod 4)，定理也就得证。

在我们刚刚考虑过的例子中，由于 $97\equiv1\pmod 4$，故有 $(-1/97)=1$.

定理 5 告诉我们，有时我们可求 -1 对模 p 的平方根：只要 $p\equiv1\pmod 4$，-1 就有一个平方根 $\pmod p$.

【练习 14】 对 3, 5, 7, 11, 13, 17, 19, 23 中哪些素数，-1 是一个二次剩余？

【练习 15】 计算 $(6/7)$ 和 $(2/23)(11/23)$.

要判定 2 是否有平方根 $\pmod p$ 却不这么容易. 欧拉准则称

$$(2/p)\equiv2^{(p-1)/2}\pmod p,$$

但是，对哪些素数来说，$2^{(p-1)/2}$ 与 1 同余 $\pmod p$？这并不明显. 我们将在下节将它们求出. 现在我们只叙述其结论：

定理 6 若 p 为奇素数，则

$$(2/p)=\begin{cases}1, & 若\ p\equiv1\ 或\ 7\pmod 8;\\ -1, & 若\ p\equiv3\ 或\ 5\pmod 8.\end{cases}$$

定理 6 以及从定理 3 到定理 5 这几个定理一起，使我们能算出任何勒让德记号的值. 例如，我们可算出 $(3201/8191)$，计算过程如下：

$$(3201/8191)=(3/8191)(11/8191)(97/8191),$$
$$(3/8191)=-(8191/3)=-(1/3)=-1,$$
$$(11/8191)=-(8191/11)=-(7/11)$$
$$=(11/7)=(4/7)=1,$$
$$(97/8191)=(8191/97)=(43/97)=(97/43)$$
$$=(11/43)=-(43/11)=-(-1/11)=1.$$

因此，我们知 $(3201/8191)=(-1)(1)(1)=-1$. 考虑我们刚才计算 $(3201/8191)$ 的工作量，并考虑用尝试法决定 $x^2\equiv3201$

(mod 8191)是否有解的工作量，将两者作一比较吧. 要计算 $1^2, 2^2, \cdots, 4095^2$，然后用 8191 逐个相除，这绝非一件轻而易举的事，定理 3 到定理 6 至少对这种事来说是一种巨大的帮助.

习　题

1. 下列同余式中哪些有解?
   (a) $x^2 \equiv 7 \pmod{53}$;　(b) $x^2 \equiv 53 \pmod{7}$;
   (c) $x^2 \equiv 14 \pmod{31}$;　(d) $x^2 \equiv 625 \pmod{9973}$.
2. 求出题 1 中有解的那些同余式的解.
3. 求解:
   (a) $x^2 + x + 1 \equiv 0 \pmod{5}$;
   (b) $x^2 + x \equiv 0 \pmod{5}$;
   (c) $x^2 + x - 1 \equiv 0 \pmod{5}$.
4. (a) $x^2 \equiv 1 \pmod{16}$有几个解?
   (b) 这与定理 1 矛盾吗?
5. 求解:
   (a) $2x^2 + 3x + 1 \equiv 0 \pmod{7}$;
   (b) $3x^2 + x + 4 \equiv 0 \pmod{7}$.
6. 设 $1 \leqslant a \leqslant 30$，哪些整数 a 是二次剩余(mod 31)?
7. 对模 23，计算：(a) 2^{11};　(b) 3^{11};　(c) 4^{11};　(d) 5^{11};　(e) 22^{11};　(f) 21^{11}.
8. 对于 $p = 3, 5, 7, 11, 13, 17$ 中哪些数，$x^2 \equiv -2 \pmod{p}$可解?
9. 计算：(a) $(33/71)$;　(b) $(34/71)$;
   (c) $(35/71)$;　(d) $(36/71)$.
10. 计算：(a) $(1234/4567)$;　(b) $(4321/4567)$.
11. 证明：若 $p = q + 4a$(p 和 q 为奇素数)，则$(p/q) = (a/q)$.
12. 证明：若对某 k，有 $p = 12k + 1$，则$(3/p) = 1$.
13. $x^2 \equiv 53 \pmod{97}$有解吗? $x^2 \equiv 97 \pmod{53}$呢?
14. 证明：定理 6 可改写为

$$(2/p)=(-1)^{(p^2-1)/8}.$$

15. 利用勒让德记号证明：三个二次非剩余 (mod p) 的乘积是一个非剩余(mod p)．两个非剩余和一个剩余的乘积是什么？
16. 有时，二次互反性定理可叙述如下：若 p 和 q 为奇素数，则

$$(p/q)(q/p)=(-1)^{(p-1)(q-1)/4}.$$

这是否是相同的定理呢？
17. 甲说："我打赌，对某一 n，7 整除 n^2+1．"乙说："我来应战．"谁将获胜呢？
18. 证明：若 a 是一个二次剩余(mod p)，$ab\equiv1$(mod p)，则 b 也是一个二次剩余(mod p)．
19. $x^2\equiv211$(mod 159)有解吗？
20. 推广题 18 的结论，找出关于 r 的条件，以保证：当 a 是二次剩余(mod p)，且 $ab\equiv r$(mod p)时，b 是二次剩余(mod p)．
21. 假定 $p=q+4a$，其中 p 和 q 为奇素数，证明：$(a/p)=(a/q)$．

§12 二次互反性

本节中，我们将证明上节叙述并使用过、但未加以证明的两个定理：二次互反性定理以及用于计算$(2/p)$的定理．它们的证明，特别是二次互反性定理的证明，是不容易的．下列结果是这两个定理的基础，它有时也称为高斯引理：

定理 1 设 p 为奇素数，$p\nmid a$，且设在

$$a,\ 2a,\ 3a,\ \cdots,\ \left(\frac{p-1}{2}\right)a$$

的各个最小剩余$(\bmod\ p)$中，恰有 g 个大于$(p-1)/2$，则 $x^2\equiv a(\bmod\ p)$ 有解还是无解取决于 g 是偶数还是奇数，换言之，$(a/p)=(-1)^g$．

在证明这一定理以前，我们取 $a=5$ 和 $p=17$ 来说明这一定理的用法．我们有$(p-1)/2=8$，且整数

$$5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ 40$$

的最小剩余$(\bmod\ 17)$分别为

$$5,\ 10,\ 15,\ 3,\ 8,\ 13,\ 1,\ 6.$$

其中有 3 个大于$(p-1)/2$．定理 1 说明，5 是二次非剩余$(\bmod\ 17)$，事实上也确是如此．

【练习 1】 应用欧拉准则，并证明 $5^8\equiv-1(\bmod\ 17)$，以验证定理 1 在上例中给出的结果是正确的．

定理 1 的证明 设 $r_1,\ r_2,\ \cdots,\ r_k$ 表示

$$a,\ 2a,\ \cdots,\ ((p-1)/2)a$$

的最小剩余$(\bmod\ p)$中小于或等于$(p-1)/2$的那些数，又设

$s_1, s_2, \cdots, s_g$ 表示它们中大于$(p-1)/2$的那些数. 因而, $k+g=(p-1)/2$. 为了证明这一定理, 只需用欧拉准则说明

$$a^{(p-1)/2}\equiv(-1)^g(\text{mod } p)$$

即可, 这也就是我们进而要做的事. (在前例中, $k=5$, $g=3$, r_i的集合为$\{5, 3, 8, 1, 6\}$, s_j的集合为$\{10, 15, 13\}$.) 在此例中, 以及在一般情况下, 任意两个r_i都不会同余$(\text{mod } p)$. 要是有两个同余, 就会有某k_1和k_2, 使

$$k_1a\equiv k_2a(\text{mod } p),\ 0\leqslant k_1\leqslant(p-1)/2,$$
$$0\leqslant k_2\leqslant(p-1)/2.$$

由于$(a, p)=1$, 故得$k_1=k_2$. 由于同样的原因, 任意两个s_j也不同余$(\text{mod } p)$. 现在, 我们来考虑数集:

(1) $$r_1, r_2, \cdots, r_k, p-s_1, p-s_2, \cdots, p-s_g.$$

这一集合中, 每个整数n都满足$1\leqslant n\leqslant(p-1)/2$, 而此集合一共有$(p-1)/2$个元素. 高斯注意到, 此集合中各数互不相同, 这一点我们马上就要证明. 因此, (1) 中所有元素恰为整数

(2) $$1, 2, \cdots, (p-1)/2$$

的一个排列, 于是(1)中元素的乘积与(2)中元素的乘积相同. 据此即可证得定理. 在我们上面考虑过的例子中, 所有r_i的集合是$\{5, 3, 8, 1, 6\}$, 所有$(p-s_j)$的集合是$\{7, 2, 4\}$; 这两个集合正好包括1到8的所有整数.

我们已经知道, 这些r_i以及s_j各自在它们内部互不相同, 所以, 为了证明(1)中元素互不相同, 我们只需证明, 对任意i和j, $r_i\not\equiv p-s_j(\text{mod } p)$. 假定对某$i$和$j$, 我们有$r_i\equiv p-s_j(\text{mod } p)$, 则$r_i+s_j\equiv0(\text{mod } p)$. 又因$r_i\equiv ta(\text{mod } p)$, $s_j\equiv ua(\text{mod } p)$, 其中$t$和$u$为小于或等于$(p-1)/2$的两个正整数, 我们应有

$$(t+u)a\equiv 0(\bmod p);$$

因$(a, p)=1$，我们有$t+u\equiv 0(\bmod p)$，这不可能，因为$2\leqslant t+u\leqslant p-1$. 所以(1)中各个元素互不相同，因而是(2)中各个元素的一个排列. 于是，

(3) $$r_1r_2\cdots r_k(p-s_1)(p-s_2)\cdots(p-s_g)$$
$$=1\cdot 2\cdot\cdots\cdot((p-1)/2).$$

由于对所有j，有$p-s_j\equiv -s_j(\bmod p)$，而这种因子共有$g$个，故(3)变为

(4) $$r_1r_2\cdots r_ks_1s_2\cdots s_g(-1)^g=\left(\frac{p-1}{2}\right)!(\bmod p).$$

但根据定义，r_1, r_2, $\cdots$, r_k, s_1, s_2, $\cdots$, s_g按某一次序恰为下列各数之最小剩余$(\bmod p)$:

$$a,\ 2a,\ \cdots,\ ((p-1)/2)a,$$

因而乘积$r_1r_2\cdots r_ks_1s_2\cdots s_g$与$a(2a)(3a)\cdots((p-1)/2)a$同余$(\bmod p)$. 于是，由(4)得

$$a^{(p-1)/2}(-1)^g\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(\bmod p).$$

上式中与p互素的公因子可以消去，得

$$a^{(p-1)/2}(-1)^g\equiv 1(\bmod p).$$

如在上式两边各乘以$(-1)^g$，得

$$a^{(p-1)/2}\equiv(-1)^g(\bmod p).$$

但我们知，$a^{(p-1)/2}\equiv(a/p)(\bmod p)$. 将最后这两个同余式合在一起，并注意到，若两数同余$(\bmod p)$，它们就应相等，我们有

$$(a/p)=(-1)^g,$$

这就是我们所要证明的事.

【练习 2】 应用上述定理判定$x^2\equiv 7(\bmod 27)$是否有解？

现在我们应用上述定理来计算p为任意奇素数时的

$(2/p)$. 根据这一定理，我们需要求出

(5) $$2,\ 4,\ 6,\ \cdots,\ 2\left(\frac{p-1}{2}\right)$$

的最小剩余$(\bmod p)$中有几个大于$(p-1)/2$. 由于(5)中各数已是最小剩余，它们都不大于p，所以我们只要看看它们中有几个大于$(p-1)/2$即可. 设第一个大于$(p-1)/2$的偶数为$2a$，则

(6) $$\frac{p-1}{2}<2a\leqslant\frac{p-1}{2}+2.$$

【练习3】 说明我们寻求的数g为

$$g=\frac{p-1}{2}-(a-1).$$

【练习4】 用(6)说明，g决定于

$$\frac{p-1}{4}\leqslant g<\frac{p-1}{4}+2.$$

【练习5】 验证下表所列各数的正确性:

p	3	5	7	11	13	17	19	23	29
g	1	1	2	3	3	4	5	6	7
$(-1)^g$	-1	-1	1	-1	-1	1	-1	1	-1.

对上表所列各数进行验证后，你就会注意到，对于哪些素数，g是偶数，对于哪些素数，g是奇数. 要是还不清楚，可假定$p\equiv1(\bmod 8)$. 则对某k，有$p=1+8k$，或$(p-1)/4=2k$. 因此，$g=2k$，g是偶数. 所以，若$p\equiv1(\bmod 8)$，则$(2/p)=1$. 类似地，若对某k，有$p=3+8k$，则$(p-1)/4=2k+1/2$，g是奇数，因此，$(2/p)=-1$.

【练习6】 检验$p=8k+5$和$p=8k+7$这两种情况.

【练习7】 我们不需要考虑$p=8k, p=8k+2, p=8k+4, p=8k+6$，为什么?

于是，我们证明了

定理 2 若 p 为奇素数，则

$$(2/p)=\begin{cases}1, & \text{当 } p\equiv 1 \text{ 或 } 7 \pmod 8 \text{ 时},\\ -1, & \text{当 } p\equiv 3 \text{ 或 } 5 \pmod 8 \text{ 时}.\end{cases}$$

我们举一个例子来应用定理 2. 我们要介绍并证明一个结果，它虽有点离题，但却逗人喜爱，也许还使人有点意外. 虽然我们知道一个数什么时候有原根存在，但要求出具体的原根，一般说来并非易事. 例如，2 是 100 以内的素数 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83 的一个原根，但 2 不是 100 以内其它素数的原根. 人们尚未证得任何定理，它能预计出以 2 作为一个原根的素数，甚至还不能证明 2 是无限多个素数的一个原根. 但是，我们有

定理 3 若 p 和 $4p+1$ 均为素数，则 2 是 $4p+1$ 的一个原根.

证明 设 $q=4p+1$，则 $\phi(q)=4p$. 故 2 的阶可能为 1, 2, 4, p, $2p$ 或 $4p \pmod q$. 我们要证，前五种情况不可能出现. 根据欧拉准则，我们有

$$2^{2p}\equiv 2^{(q-1)/2}\equiv (2/q) \pmod q.$$

但 p 是奇素数，故 $4p\equiv 4 \pmod 8$，$q\equiv 4p+1\equiv 5 \pmod 8$；由定理 2 我们知道，2 是与 5 同余 (mod 8) 的素数的一个二次非剩余，因此，

$$2^{2p}\equiv -1 \pmod 8,$$

故 2 的阶不是 $2p$，也不可能是 $2p$ 的任一因子，而 $2p$ 的因子是 1, 2, 和 p. 又因 2 的阶也不是 4 (若 $2^4\equiv 1 \pmod q$，则 $q|15$，就有 $q=5$，这是不可能的)，故定理得证.

现在我们来介绍高斯对二次互反性定理所作的第三个证

明，具有较高数学修养的人都会赞叹这种证法之巧妙完美. 它的基础就是高斯引理(定理 1) 以及我们现在即将证明的下列引理.

引理 1 若 p 和 q 为不同的奇素数，则

$$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right]$$

$$=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

记号 $[kq/p]$ 表示不大于 kq/p 的最大整数. 如对这一记号不大熟悉，可参阅附录二.

【练习 8】 对 $p=5$ 和 $q=7$, 验证引理的正确性.

引理 1 的证明 证明的思想是利用几何图形，这也是解析几何如何能使某些证明出人意外地简化的一个例子. 为了书写的方便，可令

$$S(p,\ q)=\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right].$$

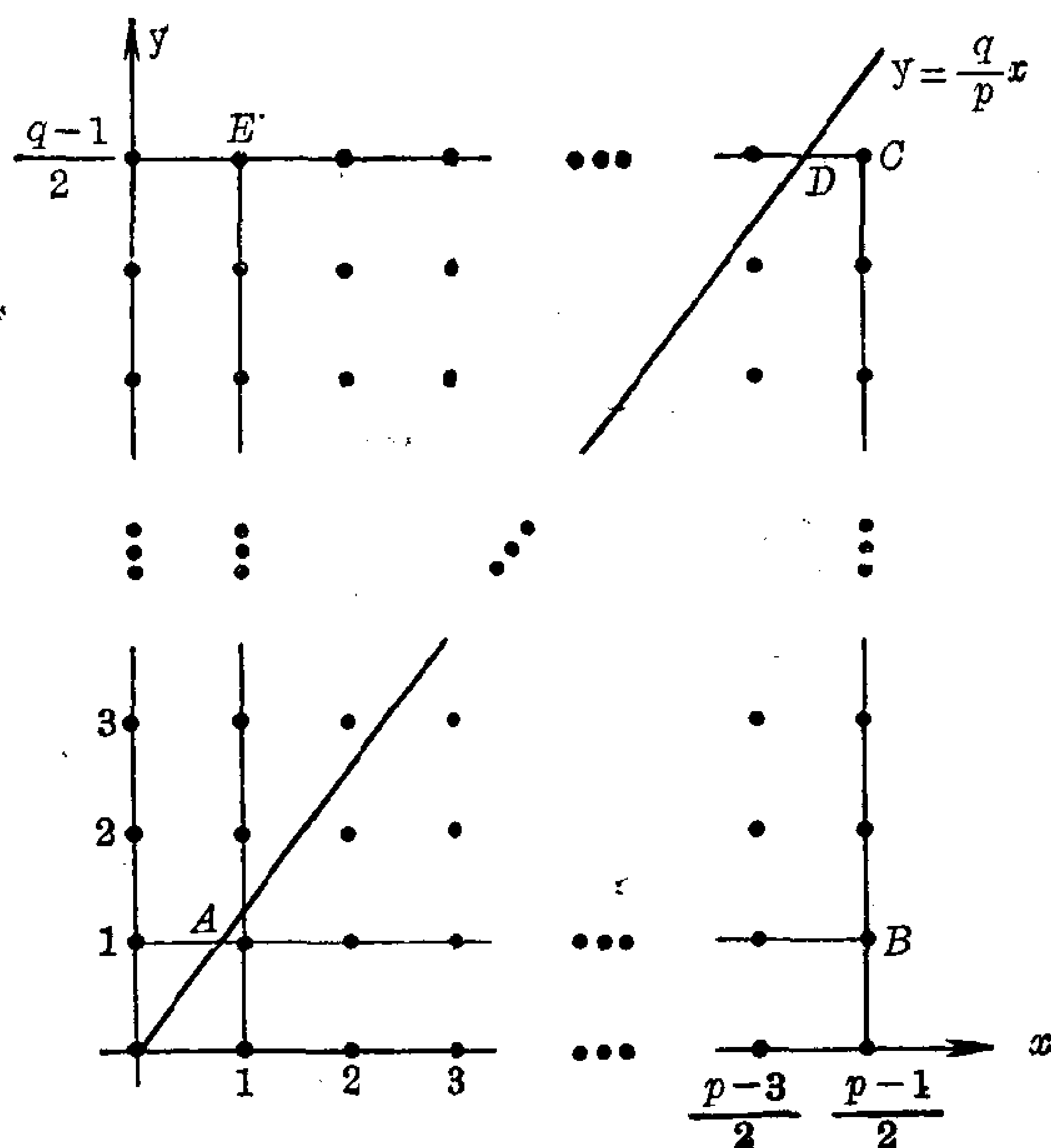
因此，我们要设法证明

$$S(p,\ q)+S(q,\ p)=(p-1)(q-1)/4.$$

在附录二中提到，$[kq/p]$ 是区间 $1<x\leqslant kq/p$ 中的整数个数，因此 $[kq/p]$ 等于位于直线 $x=k$ 上且在直线 $y=qx/p$ 下方以及直线 $y=1$ 上及其上方的格点数 (格点就是坐标为整数的点). 对于 $k=1,\ 2,\ \cdots,\ (p-1)/2$, 看一看附图我们可知

$$S(p,\ q)=\sum_{k=1}^{(p-1)/2}[kq/p]$$

就是在多边形 $ABCD$ 内部及其边界上的格点数.



同样我们知道，$S(q, p)$是多边形 ADE 内部及其边界上的格点数．由于$(q, p)=1$，故在线段 AD 上没有格点．由此可知，$S(p, q)+S(q, p)$就是以$(1, 1)$，B，C 和 E 为顶点的矩形内部及其边界上的格点数．这个数很容易算得：它等于$((p-1)/2)\cdot((q-1)/2)$，这就证明了引理．

定理 4（二次互反性定理） 若 p 和 q 为奇素数，则

$$(p/q)(q/p)=(-1)^{(p-1)(q-1)/4}.$$

注意，这与我们在前面对此定理的提法（§ 11 定理4）是等价的：若 $p\equiv q\equiv 3(\text{mod } 4)$，则$(p/q)=-(q/p)$；否则，$(p/q)=(q/p)$．这是因为，除非 $p\equiv q\equiv 3(\text{mod } 4)$，$(p-1)(q-1)/4$ 总是偶数．

证明 象在证明高斯引理时那样，让我们取

$$q,\ 2q,\ 3q,\ \cdots,\ \frac{p-1}{2}q$$

的最小剩余 (mod p)，并将它们分为两类：小于或等于 $(p-1)/2$ 的那些数归入一类，并记之为

$$r_1,\ r_2,\ \cdots,\ r_k;$$

而大于 $(p-1)/2$ 的那些数归入另一类，并记之为

$$s_1,\ s_2,\ \cdots,\ s_g.$$

因此，$k+g=(p-1)/2$. 高斯引理的结论是：$(q/p)=(-1)^g$. 为了书写方便，令

$$R=r_1+r_2+\cdots+r_k,\quad S=s_1+s_2+\cdots+s_g.$$

在证明高斯引理过程中，说明过下列一些数

(7) $$r_1,\ r_2,\ \cdots,\ r_k,\ p-s_1,\ p-s_2,\ \cdots,\ p-s_g$$

是如下各数的一个排列：

(8) $$1,\ 2,\ \cdots,\ (p-1)/2.$$

因此，(7)中各数之和与(8)中各数之和相同. 我们记得，在高斯引理的证明中，我们曾取(7)中各数之积，并使它与(8)中各数之积相等. 因而，这里存在着证明定理 4 的一个可能的出发点. 高斯可能就想过："要是我使其和相等而不是使其积相等，那么将会发生什么情况呢？"然后他就作出了证明. 不管他到底是怎样想的，有一点我们应该明白，即证明往往不是一开始就有的. 根据大家熟悉的一个公式：$1+2+\cdots+n=n(n+1)/2$（其证明见附录一），(8)中各数之和为

$$\frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)=\frac{p^2-1}{8}.$$

(7)中各数之和为

$$\sum_{j=1}^{k} r_j+\sum_{j=1}^{g}(p-s_j)=R+gp-S.$$

因而我们有

(9) $$R=S-gp+(p^2-1)/8.$$

$jq(j=1, 2, \cdots, (p-1)/2)$的最小剩余(mod p)就是jq用p相除所得之余数，我们知道商为$[jq/p]$，故当我们用t_j表示jq的最小剩余(mod p)时，就有

$$jq=[jq/p]p+t_j,\ j=1, 2, \cdots, (p-1)/2.$$

将这些式子关于j相加，我们得

$$\sum_{j=1}^{(p-1)/2} jq=\sum_{j=1}^{(p-1)/2}[jq/p]p+\sum_{j=1}^{(p-1)/2}t_j,$$

或

$$q\sum_{j=1}^{(p-1)/2} j=p\sum_{j=1}^{(p-1)/2}[jq/p]+\sum_{j=1}^{k}r_j+\sum_{j=1}^{g}s_j,$$

或

(10) $$q(p^2-1)/8=pS(p, q)+R+S.$$

将(9)代入此式，我们得

$$q(p^2-1)/8=pS(p, q)+2S-gp+(p^2-1)/8 \text{ 或}$$

(11) $$(q-1)(p^2-1)/8=p(S(p, q)-g)+2S.$$

在(11)中，左端是偶数(因为$(p^2-1)/8$是整数，$q-1$是偶数)，$2S$也是偶数，因此，余下的一项就是偶数，故$S(p, q)-g$也是偶数．因而

$$(-1)^{S(p,q)-g}=1.$$

由于$(-1)^g=(q/p)$，所以

(12) $$(-1)^{S(p,q)}=(-1)^g=(q/p).$$

现在，我们若将p和q交换一下，再重复上述论证(我们一处也未要求q具有p所没有的性质)，可得

(13) $$(-1)^{S(q,p)}=(p/q).$$

将(12)和(13)相乘，我们有

$$(-1)^{S(p,q)+S(q,p)}=(p/q)(q/p).$$

而由引理1，我们有

$$(-1)^{(p-1)(q-1)/4}=(p/q)(q/p),$$

这就是我们所要证明的结论.

习　题

1. 对课文中计算$(2/p)$所用的方法作适当修改以用来计算$(3/p)$.
2. 证明 3 是形为 4^n+1 的所有素数的一个二次非剩余.
3. 证明 3 是大于 3 的所有莫森素数 (形如 2^q-1 的素数) 的一个二次非剩余.
4. (a) 证明: 若$p\equiv 7(\bmod 8)$, 则$p\mid(2^{(p-1)/2}-1)$;
   (b) 求出$2^{83}-1$ 的一个因子.
5. (a) 若 p 和 $q=10p+3$ 均为奇素数, 证明$(p/q)=(3/p)$;
   (b) 若 p 和 $q=10p+1$ 均为奇素数, 证明$(p/q)=(-1/p)$.
6. (a) 哪些素数可以整除某个 n^2+1?
   (b) 哪些奇素数可以整除某个 n^2+n?
   (c) 哪些奇素数可以整除某个 n^2+n+2?
7. (a) 证明: 若$p\equiv 3(\bmod 4)$, 且 a 为一个二次剩余 $(\bmod p)$, 则 $p-a$ 就是一个二次非剩余$(\bmod p)$;
   (b) 若 $p\equiv 1(\bmod 4)$, 相应地应有什么结论?
8. 若 $p>3$, 证明 p 整除它的所有二次剩余之和.
9. (a) 假定 $p\geqslant 5$ 为素数, 证明: 若 $p\equiv 1$ 或$7(\bmod 12)$, 则 -3 是一个二次剩余$(\bmod p)$; 若 $p\equiv 5$ 或 $11(\bmod 12)$, 则 -3 是一个二次非剩余$(\bmod p)$;
   (b) 假定 p 为奇素数, $p\neq 3$, 且 $p\nmid a$. 又假定 $x^3\equiv a(\bmod p)$ 有一解 r, 则有
   $$(x-r)(x^2+xr+r^2)\equiv 0(\bmod p).$$
   证明: 当且仅当 $p\equiv 1$ 或 $7(\bmod 12)$ 时, $x^2+xr+r^2\equiv 0(\bmod p)$ 具有两个不同于 r 的解;
   (c) 若 $p\geqslant 5$, 证明: 不同的非零三次剩余 $(\bmod p)$ 的个数为 $p-1$ (若 $p\equiv 5$ 或 $11(\bmod 12)$) 或$(p-1)/3$(若 $p\equiv 1$ 或 $7(\bmod 12)$).
10. 若 p 为奇素数, 计算
    $$(1\cdot 2/p)+(2\cdot 3/p)+\cdots+((p-2)(p-1)/p).$$
11. 证明: 若 $p\equiv 1(\bmod 4)$, 则 $x^2\equiv -1(\bmod p)$ 有一解等于$((p-1)/2)!$的最小剩余$(\bmod p)$.

§13 用不同的基表示的数

发明我们熟悉的书写整数的记号，是人类智慧的一大创造，也是数学能够产生的一个条件. 我们书写整数所用的记号是位置与数值的综合，不同的位置表示着10的不同的乘幂. 例如，

$$314,159=3\cdot10^5+1\cdot10^4+4\cdot10^3+1\cdot10^2+5\cdot10^1+9\cdot10^0.$$

我们没有理由认为某一不同于10的整数就不能用于同样的目的，而取10也只不过是出于人体结构这一偶然因素. 事实上，其它整数(我们称它们为基)在过去也曾使用过. 3,000年前的巴比伦人有时就用60做基，古代马雅人用20做基. 今天，计算机所用的数是以2，8和16为基来表示的. 本节中，我们要考察一下不用10作基的整数.

我们首先来看一种特殊的情况.

定理1 每个正整数都可写为2的不同乘幂的和.

例如，$22=2^4+2^2+2^1$，$23=2^4+2^2+2^1+2^0$；但 $24=2^3+2^3+2^3$ 不是正确的表示式，因为其中2的各个乘幂都是相同的.

【练习1】 把31和33写成2的不同乘幂的和.

定理1的证明 证明的思想是：取一个正整数 n，从中减去不大于它的2的最大乘幂，比方说是 2^k，然后对 $n-2^k$ 也这样做，如此继续做下去，我们最终定能将 n 表示成我们所需的形式. 说得严格一点，我们是用归纳法证明这个定理的.

$1=2^0$, $2=2^1$, $3=2^0+2^1$, 故定理对 1, 2, 3 这些整数成立. 现在假定, 每个整数 k, $k\leqslant n-1$, 都能写成 2 的不同乘幂的和, 我们要证 n 也可这样表出. 我们知, n 一定位于 2 的某两个不同乘幂之间, 也即存在一个整数 r, 使

(1) $$2^r\leqslant n<2^{r+1}.$$

【练习 2】 若 $n=74$, r 是什么数? 若 $n=174$, r 是什么数?

2 的不大于 n 的最大乘幂是 2^r. 令 $n'=n-2^r$, 则 $n'\leqslant n-1$. 故归纳法假设告诉我们, 它可以写为 2 的不同乘幂之和:

$$n'=2^{e_1}+2^{e_2}+\cdots+2^{e_k},$$

其中若 $i\neq j$, 则 $e_i\neq e_j$. 由于 $n'=n-2^r$, 我们有

(2) $$n=2^r+2^{e_1}+2^{e_2}+\cdots+2^{e_k},$$

所以 n 就写成了 2 的乘幂之和. 要完成证明, 我们还需说明, r 与 e_1, e_2, $\cdots$, e_k 中任一数都不相同.

【练习 3】 这是为什么?

我们现在证明, 表示式(2)是唯一的.

定理 2 每一正整数可以唯一地写为 2 的不同乘幂之和.

证明 假定 n 写为 2 的不同乘幂之和的表示式有两个, 我们要证明这两个表示式实际上是相同的. 为了使记号不那么累赘, 我们注意到, 任何 2 的不同乘幂之和都可写成如下的形式:

(3) $$d_0+d_1\cdot 2+d_2\cdot 2^2+d_3\cdot 2^3+\cdots+d_k\cdot 2^k,$$

其中 k 为某整数, 且对每一 i, 有 $d_i=0$ 或 1. 反过来, 每个这样的和都是 2 的不同乘幂之和. 因此, 将 n 写成(2)的形式或(3)的形式并不重要, 但(3)有它的优点, 它的各个幂指数由小

到大依次排列，故不必再配上足标．若 n 有两种表示式，设为

(4) $$n=d_0+d_1\cdot 2+d_2\cdot 2^2+\cdots+d_k\cdot 2^k$$
$$=e_0+e_1\cdot 2+e_2\cdot 2^2+\cdots+e_k\cdot 2^k,$$

其中对每一 i，有 $d_i=0$ 或 1，$e_i=0$ 或 1．（注意，我们假定了两个表示式的项数相同，这并不失去一般性，若一个表示式比另一个表示式来得长，那么我们可在较短的那个表示式中加入一些等于零的项使它们一样长．）从(4)的第一个表示式中减去第二个表示式，得

(5) $$0=(d_0-e_0)+(d_1-e_1)\cdot 2+(d_2-e_2)\cdot 2^2+\cdots$$
$$+(d_k-e_k)\cdot 2^k.$$

因此，$2|(d_0-e_0)$．但因 d_0 和 e_0 都是 0 或 1，故有

$$-1\leqslant d_0-e_0\leqslant 1.$$

而 2 在这一范围内的倍数只有 0，故 $d_0=e_0$．因此(5)中第一项消失，我们可用 2 去除留下的两端，得

(6) $$0=(d_1-e_1)+(d_2-e_2)\cdot 2+\cdots+(d_k-e_k)\cdot 2^{k-1}.$$

与前面同样的论证可以说明，$d_1=e_1$．在 (6) 中丢掉 d_1-e_1，用 2 相除，再次使用与上述同样的论证，我们得 $d_2=e_2$．如此继续下去，可得 $d_3-e_3=d_4-e_4=\cdots=d_k-e_k=0$，从而 (4) 中两个表示式相同．

定理 1 和定理 2 说明，每一 n 恰有一种方式写成如下的形式：

(7) $$d_0+d_1\cdot 2+d_2\cdot 2^2+d_3\cdot 2^3+\cdots+d_k\cdot 2^k,$$

其中 k 为某一数，每个 d_i 都是 0 或 1．这与整数的普通十进位表示式相象，而且是如此相象，以致我们可将 (7) 这种形式的数用我们平常写整数的同一格式写出．由于决定着 n 的值的是数列 $d_0, d_1, \cdots, d_k$，而 (7) 中那些 2 的乘幂和加号却并不重要，因此我们可将表示式(7)写成

(8) $$(d_k d_{k-1} \cdots d_1 d_0)_2,$$

并称这个整数已用基 2 写出．足标 2 提醒我们，d_r 应乘上 2^r．例如，

$$101001_2 = 1+0\cdot2+0\cdot2^2+1\cdot2^3+0\cdot2^4+1\cdot2^5$$
$$=1+8+32=41.$$

而在另一方面，则有

$$94=64+16+8+4+2$$
$$=1\cdot2^6+0\cdot2^5+1\cdot2^4+1\cdot2^3+1\cdot2^2+1\cdot2^1+0\cdot2^0$$
$$=1011110_2.$$

【练习 4】 计算 1001_2, 111_2, 1000000_2.

【练习 5】 将 2, 20, 200 用基 2 写出．

我们知道，每个整数可唯一地表示为如下形式：

$$d_0+d_1\cdot10+d_2\cdot10^2+\cdots+d_k\cdot10^k,$$

其中 k 为某数，且 $0\leqslant d_i<10$, $i=0, 1, \cdots, k$. 而定理 1 和定理 2 说明，每个整数也可唯一地表示为如下的形式：

$$d_0+d_1\cdot2+d_2\cdot2^2+\cdots+d_k\cdot2^k,$$

其中 k 为某数，且 $0\leqslant d_i<2$, $i=0, 1, \cdots, k$. 对 2 和 10 我们能做到的事，对其它大于 1 的整数，我们也应能够做到．事实上，我们可以证明下列定理：

定理 3 设 $b\geqslant2$ 为任一整数(称为基)，任一正整数可唯一地用基 b 来表示，即可写为如下的形式：

(9) $$n=d_0+d_1\cdot b+d_2\cdot b^2+\cdots+d_k b^k,$$

其中 k 为某数，且 $0\leqslant d_i<b$, $i=0, 1, \cdots, k$.

证明 我们将首先证明，每一整数都有这样一个表示式，然后证明，这种表示式是唯一的．为了证明存在着一个表示式，我们本来只要将定理 1 的证明作相应修改即可，但我们在这里介绍另一证法（它也适用于定理 1)，它还能给出 n 以 b

为基时的各位数字来．用 b 除 n，除法算式给出

$$n=q_1b+d_0,\ 0\leqslant d_0<b.$$

可再用 b 去除商，得

$$q_1=q_2b+d_1,\ 0\leqslant d_1<b,$$

如此继续下去，得

$$q_2=q_3b+d_2,\quad 0\leqslant d_2<b,$$

$$q_3=q_4b+d_3,\quad 0\leqslant d_3<b,$$

等等．因 $n>q_1>q_2>q_3>\cdots$，且每个 q_i 非负，这些 q_i 组成的序列迟早终将中断，也就是说，我们将遇到一个 k，使

$$q_k=0\cdot b+d_k,\ 0\leqslant d_k<b.$$

然而，这样就有

$$\begin{aligned}n&=d_0+q_1b=d_0+(d_1+q_2b)b=d_0+d_1b+q_2b^2\\&=d_0+d_1b+(d_2+q_3b)b^2=d_0+d_1b+d_2b^2+q_3b^3\\&=\cdots=d_0+d_1b+d_2b^2+\cdots+q_kb^k\\&=d_0+d_1b+d_2b^2+\cdots+d_kb^k,\end{aligned}$$

这就是欲求之表示式．

要证明这种表示式是唯一的，可用证明定理 2 时所用的思想．假定 n 有两种表示式：

$$\begin{aligned}n&=d_0+d_1b+d_2b^2+\cdots+d_kb^k\\&=e_0+e_1b+e_2b^2+\cdots+e_kb^k,\end{aligned}$$

其中 k 为某数，且对于 $i=0,\ 1,\ \cdots,\ k$，有

(10) $$0\leqslant d_i<b,\ 0\leqslant e_i<b.$$

(正如定理 2 中说过的那样，假定这两种表示式的项数相同并不失去一般性．)将一个表示式从另一个中减去，得

$$\begin{aligned}0=&(d_0-e_0)+(d_1-e_1)b\\&+(d_2-e_2)b^2+\cdots+(d_k-e_k)b^k.\end{aligned}$$

我们知，$b\mid(d_0-e_0)$，由(10)可得 $d_0=e_0$．

【练习 6】 完成这一定理的证明.

为简便起见，我们可以这样写：

$$d_0+d_1b+\cdots+d_kb^k=(d_kd_{k-1}\cdots d_1d_0)_b.$$

例如，$111_7=1+1\cdot7+1\cdot7^2=57_{10}$.（当 $b=10$ 时，我们通常将足标省去. 除非另有说明，没有足标的整数就是以 10 为基写出的.）

为了求出一个十进位数用 b 做基时的表示式，最好是用定理 3 的证明中所用的格式. 例如，要将 31415 以 8 为基写出，我们可重复地用 8 相除：

$$31415=8\cdot3926+7,$$
$$3926=8\cdot490+6,$$
$$490=8\cdot61+2,$$
$$61=8\cdot7+5,$$
$$7=8\cdot0+7,$$

因此，$31415_{10}=75267_8$.（验算：$75267_8=7+6\cdot8+2\cdot8^2+5\cdot8^3+7\cdot8^4=7+48+128+2560+28762=31415$.）

为了算起来方便些，可将除法换一种格式排起来. 例如，我们有 $31415_{10}=160406_7$：

商	余数
7)31415	
4487	6
641	0
91	4
13	0
1	6
0	1

习 题

1．以下列数为基写出1492：(a) 2；(b) 3；(c) 7；(d) 9；(e) 11.

2．计算：(a) 3141_5；(b) 3141_6；(c) 3141_7；(d) 3141_9.

3．求出x：(a) $123_4=x_5$；(b) $234_5=x_6$；(c) $123_x=1002_4$.

4．验证在下列以7为基的加法表中列出的数是正确的，并完成此表.

+	1	2	3	4	5	6	10
1	2	3	4	5	6	10	11
2	3	4	5	6	10	11	12
3	4	5	6	10	11	12	13
4	5	6	10	11	12	13	14
5							
6							
10							

5．验证在下列以7为基的乘法表中列出的数是正确的，并完成此表.

·	2	3	4	5	6	10
2	4	6	11	13	15	20
3	6	12	15	21	24	30
4	11	15	22	26	33	40
5						
6						

6．本题中所有数均以7为基，计算：

(a) $15+24+33$；(b) $314+152+265+351$；

(c) $42\cdot12$；　　(d) $314\cdot152$.

7．将下列各数写成十进位分数：

(a) $(.25)_7$；(b) $(.333\cdots)_7$；(c) $(.545454\cdots)_7$.（$(.d_1d_2d_3\cdots)_b$的含义是$d_1/b+d_2/b^2+d_3/b^3+\cdots$.）

8．b为哪些数时，1111_b可被5整除？

9. (a) 证明：123_7, 132_7, 312_7, 231_7, 321_7, 213_7 均为偶数;

(b) 证明：以7为基时，一个整数是偶数的充要条件是它的各位数字之和为偶数;

(c) 以哪些数为基时，下列结论成立：若一个整数为偶数，则以它的各位数字所作的任一排列也是偶数?

10. (a) 证明：$121_3=4^2$, $121_4=5^2$, $121_5=6^2$;

(b) 猜想并证明一个定理;

(c) 以10为基，计算 169_b 的值 $(b\geqslant 10)$.

11. 若 a 和 b 为正整数，则 a^2 必定以偶数个零结尾，$10b^2$ 必定以奇数个零结尾. 由此，对非零整数，不可能成立 $10b^2=a^2$. 由此可知，$10^{1/2}$ 是无理数.

(a) 当整数以 b(b 不是一个平方数)为基时，修改上述论证，以说明 $b^{1/2}$ 是无理数;

(b) 用同样的论证说明 $b^{1/m}$(b 不是一个 m 次幂，$m=3, 4, \cdots$) 是无理数.

12. 考虑下列几张表:

表 1

1	9	17	25
3	11	19	27
5	13	21	29
7	15	23	31

表 2

2	10	18	26
3	11	19	27
6	14	22	30
7	15	23	31

表 4

4	12	20	28
5	13	21	29
6	14	22	30
7	15	23	31

表 8

8	12	24	28
9	13	25	29
10	14	26	30
11	15	27	31

表 16

16	20	24	28
17	21	25	29
18	22	26	30
19	23	27	31

从1到31中任取一数，看一看它在哪些表上出现. 如果你把有此数出现的那些表的表号 (即1, 2, 4, 8或16) 相加，就会得到你所取的那个数. 这一戏法的诀窍在哪儿?

13. 证明：每个正整数均可唯一地写为如下的形式:

$$n=e_0+3e_1+3^2e_2+3^3e_3+\cdots+3^ke_k,$$

其中 k 为某数，$e_i=-1$，0 或 1，$i=0, 1, \cdots, k$.

14. 一个古怪的人答应赠送 100,000 元. 说他古怪是因为，他一定要使分出的每份赠款包含的元数都是 2 的乘幂，且每种数量只给一份，他应怎样来分这笔赠款呢？

15. (a) 证明：每个正奇数都可以表为如下的形式：

$$n=d_0+d_1\cdot 2+d_2\cdot 2^2+\cdots+d_k\cdot 2^k$$

其中 $d_i=1$ 或 -1，$i=0, 1, \cdots, k$，但这种表示式不是唯一的；

(b) 甲和乙赌赙，第一局赌注是 1 元，第二局是 2 元，如此等等，每局赌注都是前一局的 2 倍. 赌了 8 局后，甲赢得 31 元，他赢了哪几局？

16. 如果一个天平的两个盘子上均允许放置砝码，为了称出重量为 1 磅，2 磅，……，100 磅的物件，需要的砝码的最小个数是多少？

§14 十二进位数

本节中，我们要详细研究一下十二进位数的算术. 为此，我们要在一种陌生的结构中重新考察大家熟悉的加减乘除四则运算. 你做完本节中的练习后，就会体会到，对于十进位数的计算，你在实际上已经是多么熟练，而要学会迅速地进行算术运算，该要付出多么艰巨的劳动！要进行练习，除了可用 12 做基外，用其它的基也是可以的，但对算术中的某些内容(特别是小数)，用 12 做基要比用 10 做基更好些. 此外，在日常生活中也可碰到许许多多的"12"：物品用"打"(12 个)和"箩"(12 打)来计数，一年中有 12 个月，一英尺有 12英寸，一码是 12 英尺的一半，一天是两个 12 小时，一个圆周角是三十个 12 度. 存在着那么多的"12"，其原因在于：12 很容易地可被 3, 4 和 6 整除，而我们对这类除法的需要，比对用 5 去除什么数的需要更为经常些. 用十进制计数实在是一种令人遗憾的偶然性结果；要是我们每只手有六个手指的话，这个世界将会变得多么有条不紊啊！尽管用十二进制计数的优越性十分明显，但因为我们每只手没有六个手指，看来我们永远也不会抛弃用十进制计数的做法了. 不过，仍有一个"美国十二进制学会"在作十二进制的推广工作.

为了用十二进制计数，我们需要两个新的数字来代表 10_{10} 和 11_{10}. 本节中，从现在开始，对足标若未另加说明，所有的数都是十二进位数，即以 12 为基写出的数. 十二进位数专家们为 10_{10} 和 11_{10} 已经定下的记号看来是希腊字母 χ 和

ε, 但要读为“台”(dec)和“厄”(el)[注]. 因此, 用十二进制计数时, 有

$$1, 2, 3, 4, 5, 6, 7, 8, 9, \chi, \varepsilon, 10,$$
$$11, \cdots, 1\chi, 1\varepsilon, 20, \cdots, 30, \cdots, 40,$$
$$\cdots, \chi 0, \cdots, \varepsilon 0, \cdots, 100, \cdots.$$

用十二进位数还需要一些名称. “十二进制学会”主张用“打”表示10, 用“箩”表示100. 因此, 举例来说, 15就是“打五”, 327就是“三箩二打七”. 该学会还为“一打”的大倍数和小倍数确定了名称, 下面我们举例列出一打这样的名称:

10	打(Do)	.1	点打(Edo)
100	箩(Gro)	.01	点箩(Egro)
1000	莫(Mo)	.001	点莫(Emo)
10, 000	打莫(Do-mo)	.0001	点打莫(Edo-mo)
100, 000	箩莫(Gro-mo)	.00001	点箩莫(Egro-mo)
1, 000, 000	皮莫(Bi-mo)	.000001	点皮莫(Ebi-mo)

不巧得很, 这些名称听起来倒很象孩子们的呀呀学语声. (2, 201, 110这个数读起来就是“二皮莫, 二箩莫, 莫, 箩, 打”, 但.37χ5应读成“点三七台五”.)

十二进位数的加法不难, 只要记住, 每当我们加满一打时, 就要进一. 下面是关于6的加法表:

6	6	6	6	6	6	6	6	6	6	6	6
1	2	3	4	5	6	7	8	9	χ	ε	10
7	8	9	χ	ε	10	11	12	13	14	15	16.

而这里有几个加法运算:

[注] 在十二进制数中引进的新名称, 除“打”(dozen)和“箩”(gross)外, 均未查到统一的译名, 这里大部分采用音译. ——译校者注

$$\begin{array}{r}5\\4\\3\\2\\\hline 12\end{array}\qquad\begin{array}{r}31\\41\\15\\9\\\hline 94\end{array}\qquad\begin{array}{r}123\\456\\789\\\chi\varepsilon 0\\\hline 2036\end{array}\qquad\begin{array}{r}\chi\chi\chi\\\varepsilon\varepsilon\varepsilon\\\chi\varepsilon\chi\\\varepsilon\chi\varepsilon\\\hline 3996.\end{array}$$

【练习 1】 计算：$9+4$, $\chi+\varepsilon$, $\varepsilon 1+1\varepsilon$, $16+19+37$.

尽管在脑子里要记住加法表不太困难，但我们在做乘法时还需要一张乘法表以供查阅，这和我们以前学做以 χ 为基的数的乘法时情况一样.

十二进位数乘法表

·	2	3	4	5	6	7	8	9	χ	ε	10
2	4	6	8	χ	10	12	14	16	18	1χ	20
3	6	9	10	13	16	19	20	23	26	29	30
4	8	10	14	18	20	24	28	30	34	38	45
5	χ	13	18	21	26	2ε	34	39	42	47	50
6	10	16	20	26	30	36	40	46	50	56	60
7	12	19	24	2ε	36	41	48	53	5χ	65	70
8	14	20	28	34	40	48	54	60	68	74	80
9	16	23	30	39	46	53	60	69	76	83	90
χ	18	26	34	42	50	5χ	68	76	84	92	$\chi 0$
ε	1χ	29	38	47	56	65	74	83	92	$\chi 1$	$\varepsilon 0$

【练习 2】 验证上述乘法表中关于与 χ 相乘的部分是正确的.

借助此表，做乘法应不成问题. 例如，

$$\begin{array}{r}34\\5\\\hline 148\end{array}\qquad\begin{array}{r}1755\\\chi\\\hline 14262\end{array}\qquad\begin{array}{r}\chi\chi\\\varepsilon\varepsilon\\\hline 9\varepsilon 2\\9\varepsilon 2\\\hline \chi 912\end{array}$$

【练习 3】 计算：14·2, 14·3, 9·χ·ε.

做了足够数量的练习，我们就能把乘法表记住并学会不查表做乘法；到后来就会全凭条件反射得知"九乘九"是"六打九".

除法却要困难一些，即使有乘法表的帮助也是如此，这是因为，我们在求一个商中的数字时，如缺乏经验就可能选错．要学会一眼看出 763 中有多少个 χ5，这需要多做练习．

【练习 4】 763 中有多少个 χ5？

这里是几个算好的除法：

```
5)456|χ8        22)456|20        31)4159|140
  42               44               31
   36              16               105
   34                               104
    2                                 19
```

【练习 5】 计算 1966/6 和 1111/5.

在十二进位数制中，1/3 和 1/6 展开后是有限小数：1/3 =4/10= .4，1/6=2/10= .2，这与以 χ 为基的情况相比，是一更为可喜的现象．然而，1/5 展开成小数时，却不是有限的了：

```
     .2497
  5 )1.0000
     χ
     20
     18
      40
      39
       30
       2ε
        1
```

因此，1/5= .24972497…．我们可在循环小数的循环部分上

面加上一横，从而我们可记 $1/5=.\overline{2497}$. 诚然，对这种数用另一名称（"十二进小数"）可能更为合适，但我们仍把它们称为"小数"。

【练习 6】 将 1/7 表示为小数.

下面是一张倒数表，所列倒数一直包括到台分之一和厄分之一：

n	2	3	4	5	6	7	8	9	χ	ε
$1/n$	.6	.4	.3	$.\overline{2497}$	.2	$.\overline{186\chi35}$	.16	.14	$.\overline{12497}$	$.\overline{1}$

其中一半是有限小数，且厄分之一与十进制中的九分之一一样，循环部分特别简单.

将小数化为分数，我们使用的方法与以 χ 为基时相同. 例如，$.25=25/100$. 这一分数是最简分数吗？实际上，它的分子和分母均不能被 5 整除. 由于我们对十二进位数还不大熟悉，要认出公因子或看出没有公因子，也许有些困难. 下面是一张简短的因子分解表：

2 素数	11 素数	$21=5^2$
3 素数	$12=2\cdot7$	$22=2\cdot11$
$4=2^2$	$13=3\cdot5$	$23=3^2$
5 素数	$14=2^4$	$24=2^2\cdot7$
$6=2\cdot3$	15 素数	25 素数
7 素数	$16=2\cdot3^2$	$26=2\cdot3\cdot5$
$8=2^3$	17 素数	27 素数
$9=3^2$	$18=2^2\cdot5$	$28=2^5$
$\chi=2\cdot5$	$19=3\cdot7$	$29=3\cdot\varepsilon$
ε 素数	$1\chi=2\cdot\varepsilon$	$2\chi=2\cdot15$
$10=2^2\cdot3$	1ε 素数	$2\varepsilon=5\cdot7$
	$20=2^3\cdot3$	$30=2^2\cdot3^2$

由于 25 是一素数，故知 25/100 已是最简分数.

循环小数也可用通常的办法化为分数. 例如, 设 $N=.6666\cdots$, 则 $10N=6.666\cdots$, 故 $10N-N=6$, $\varepsilon N=6$, $N=6/\varepsilon$, 它已是一个最简分数.

习　题

1. 将课文中的因子分解表扩充至40.
2. 计算: (a) $3141+5926$; (b) $3141-5926$;
   (c) $3141\cdot5926$; (d) $3141/5926$(精确至三位小数).
3. 计算: (a) 2^{10}; (b) $9!$; (c) $1/3^3$.
4. 证明: $.292929\cdots=3/11$.
5. 取你的年龄, 加11, 乘以2, 再乘6并减去110. 证明你算得的数是你年龄的10倍.
6. $4\varepsilon.\varepsilon6$ 元和 $(59.95)_\chi$ 元, 哪个数目大?
7. 若 x 为 0, 1, 4 或 9, 证明: 当 $n=2, 3, \cdots$ 时, x^n 的末位数是 x.
8. 证明一个平方数的末位数为 0, 1, 4 或 9.
9. 证明: 当 $n=2, 3, \cdots$ 时,
   (a) 若 $x=6$, 则 x^n 的末位数是 0;
   (b) 若 $x=\chi$, 则 x^n 的末位数是 4;
   (c) 若 $x=3, 5, 7, 8, \varepsilon$, 且 n 为奇数, 则 x^n 的末位数是 x.

χ. 根据题7、题8和题9推证: 当 $n=2, 3, \cdots$ 时, 对任何 x, x^n 的末位数不可能是 2, 6, χ.

ε. 一个素数的末位数可能是哪些数?

10. 证明: 末位数是 3, 6, 9, 0 的任何整数都具有因子 3.
11. 证明: 末位数是 4, 8, 0 的任何整数都有因子 4, 末位数是 6 或 0 的任何整数都有因子 6.
12. (a) 以下各式对不对? $19^2=361$, $21^2=441$, $23^2=529$.
    (b) 你能解释(a)中出现的现象吗?
13. 5, 15, 25, 35, 45 均为素数, 再下去仍能这么说吗?
14. 将下列各数写成最简分数: (a) 3.14; (b) $.090909\cdots$.
15. 将下列各数写成循环小数: (a) 22/7; (b) 1/11.
16. 求 $2^{1/2}$, 精确到两位小数.

17. 证明：各位数字之和是 ε 的任一整数可为 ε 整除.

18. 利用 $1001=7\cdot11\cdot17$，提出整数能被 7，11 和 17 整除的各自的判别方法.

19. "美国十二进制学会"还主张使用十二进制的度量衡制度：1000 码为 1 英里，10 唡为 1 磅，10 弗朗司为 1 品脱. 该学会规定了距离、重量和体积之间的关系，要求 1 立方码可装 1000 品脱的水，而它的重量应为 1000 磅. 如果我们保持现在所用的"码"，那么十二进制度量衡制度中的英里、品脱和磅与普通的英里、品脱和磅有没有区别？

1χ. (a) 一年里有多少天？

(b) 还有哪些三位数与上述数有同样的性质：即

$$d_1d_2d_3=((d_1+1)d_2d_3)_\chi?$$

(c) 有没有四位数也有此性质？

§15 十进位小数

有些分数的小数展开式是十分良好的（如 $1/8=0.125$）；有些则较差，但还算可以（如 $1/3=0.333\cdots$）；而另外一些就很糟糕了（如 $1/17=0.0588235294117647\cdots$）. 本节中，我们要研究一下，哪些分数是良好的，并要找出一种方法来，它能决定一个循环小数的循环部分有多长，但用不着实际去计算这个小数. 为了做到这一点，除了要用到除法算式和一些同余式外，不需要用任何其它更加深奥的知识.

我们将用 $.d_1d_2d_3\cdots$ 来记

$$d_1/10+d_2/10^2+d_3/10^3+\cdots \quad (0\leqslant d_k<10).$$

一个小数的某一部分上面加一横，表示这一部分要无限地重复出现. 例如，

$$.0\overline{147}=.0147474747\cdots;\quad 1/3=.\overline{3}.$$

【练习 1】 将 $.0\overline{147}$ 写成一个分数.

【练习 2】 将 $7/41$ 写成小数，并在循环部分上面加横.

我们来为开头几个整数的倒数的小数展开式造一张表，并看一看能否从中觉察到某种规律. 在此表中，在"循环节长"这一列中的"0"表示此倒数是有限小数.

此表中，倒数是有限小数的整数有

$$2,\ 4,\ 5,\ 8,\ 10,\ 16,\ 20,\ 25,$$

这些数有一个共同点，即它们的形式都是 2^a5^b，其中 a 和 b 是一些非负整数. 我们可以猜想，具有这种形式的任一数，其倒

n	$1/n$	循环节长	n	$1/n$	循环节长
2	$.5$	0	16	$.0625$	0
3	$.3$	1	17	$.\overline{0588235294117647}$	16
4	$.25$	0	18	$.0\overline{5}$	1
5	$.2$	0	19	$.\overline{052631578947368421}$	18
6	$.1\overline{6}$	1	20	$.05$	0
7	$.\overline{142857}$	6	21	$.\overline{047619}$	6
8	$.125$	0	22	$.0\overline{45}$	2
9	$.\overline{1}$	1	23	$.\overline{0434782608695652173913}$	22
10	$.1$	0	24	$.041\overline{6}$	1
11	$.\overline{09}$	2	25	$.04$	0
12	$.08\overline{3}$	1	26	$.0\overline{384615}$	6
13	$.\overline{076923}$	6	27	$.\overline{037}$	3
14	$.0\overline{714285}$	6	28	$.03\overline{571428}$	6
15	$.0\overline{6}$	1	29	$.\overline{0344827586206896551724137931}$	28

数必能展开成有限小数．接下去三个这样的数是32, 40, 50，且

$$1/32=.03125,\quad 1/40=.025,\quad 1/50=.02$$

全是有限小数．事实上，上述猜想是正确的．

定理1 若 a 和 b 为任意非负整数，则 $1/2^a5^b$ 的小数展开式是有限的．

证明 设 M 是 a 和 b 中较大者，则

$$10^M(1/2^a5^b)=2^{M-a}5^{M-b}$$

是一个整数，把它称为 n．显然，$n\leqslant 10^M$．因此，

$$\frac{1}{2^a5^b}=\frac{n}{10^M},$$

故 $1/2^a5^b$ 的小数展开式中包括了 n 的各位数字，前面可能还有几个零．

【练习 3】 对 16, 20, 25 算出 M, 与前表作一比较, 以说明 M 正确地给出了小数展开式的长度.

【练习 4】 1/128, 1/320, 1/800 的小数展开式中各有几位?

定理 1 的逆定理也是成立的.

定理 2 若 $1/n$ 具有有限小数展开式, 则 $n=2^a5^b$, 其中 a 和 b 为某两个非负整数.

证明 设 $1/n$ 展开成有限小数为

$$1/n=.d_1d_2\cdots d_k$$
$$=d_1/10+d_2/10^2+\cdots+d_k/10^k.$$

那么, $$1/n=(d_110^{k-1}+d_210^{k-2}+\cdots+d_k)/10^k.$$

将括号内的整数称为 m, 则上式为

$$1/n=m/10^k, \text{ 或 } mn=10^k.$$

10^k 的素因子只有 2 和 5, 故 n 的素因子也只有 2 和 5, 定理得证.

定理 1 和定理 2 说的全是有限小数. 在前表中, 有些展开出来的无限小数的循环节长较大, 如 $n=17, 19, 23, 29$ 等. 这几个无限小数相应的 n 均为素数, 且 $1/n$ 的循环节长是 $n-1$. 但是, 并非所有素数 p 的倒数的循环节长都是 $p-1$, 如 1/13 的循环节长是 6, 不是 12; 1/11 的循环节长是 2, 不是 10. 作为研究倒数的循环节长的第一步, 我们证明

定理 3 在 $1/n$ 的十进位小数展开式中, 循环节长必不大于 $n-1$.

证明 设 t 满足 $10^t<n\leqslant 10^{t+1}$, 则反复利用除法算式, 我们有

$$
(1)\quad \begin{array}{ll}
10^{t+1}=d_1n+r_1, & 0\leqslant r_1<n,\\
10r_1=d_2n+r_2, & 0\leqslant r_2<n,\\
10r_2=d_3n+r_3, & 0\leqslant r_3<n,\\
\cdots, & \cdots,\\
10r_k=d_{k+1}n+r_{k+1}, & 0\leqslant r_{k+1}<n,\\
\cdots, & \cdots,
\end{array}
$$

注意，每一 d_k 都小于 10，这是因为：若 $k=1$，则

$$d_1n=10^{t+1}-r_1\leqslant 10^{t+1}=10\cdot 10^t<10n;$$

若 $k=2, 3, \cdots$，则

$$d_kn=10r_{k-1}-r_k\leqslant 10r_{k-1}<10n.$$

由(1)，我们知，

$$(2)\qquad r_k/n=d_{k+1}/10+r_{k+1}/10n.$$

如果我们用 $10^{t+1}n$ 去除(1)之第一式，并反复应用(2)，我们得

$$
\begin{aligned}
1/n&=d_1/10^{t+1}+r_1/(n10^{t+1})\\
&=d_1/10^{t+1}+d_2/10^{t+2}+r_2/(n10^{t+2})\\
&=d_1/10^{t+1}+d_2/10^{t+2}+d_3/10^{t+3}+r_3/(n10^{t+3})\\
&=\cdots\\
&=d_1/10^{t+1}+d_2/10^{t+2}+d_3/10^{t+3}+d_4/10^{t+4}+\cdots,
\end{aligned}
$$

所以，$d_1, d_2, d_3, \cdots$ 就是 $1/n$ 展成的小数的各位数字．例如，对于 $n=7$，我们有

$$
\begin{aligned}
10&=1\cdot 7+3,\\
30&=4\cdot 7+2,\\
20&=2\cdot 7+6,\\
60&=8\cdot 7+4,\\
40&=5\cdot 7+5,\\
50&=7\cdot 7+1,\\
10&=1\cdot 7+3,\\
&\cdots,
\end{aligned}
$$

故 1/7 展成小数是 $.\overline{142857}$.

余数 $r_1, r_2, \cdots$ 中，每一个都可取 $0, 1, 2, \cdots, n-1$ 这 n 个值中的某一个，因此在 $r_1, r_2, \cdots, r_{n+1}$ 这 $n+1$ 个整数中，必有两个相等.（如果你将 $n+1$ 个物体放置于 n 个盒子中，必有一个盒子装有两个或两个以上的物体.）若 $r_j = r_k$，则由 (1) 得，$d_{k+1}=d_{j+1}, d_{k+2}=d_{j+2}, \cdots$，故知这是一个循环小数，且循环节长不大于 n[注].

【练习 5】 使用除法算式将 1/41 展成小数.

若 n 与 10 互素，关于 $1/n$ 的循环节长我们还可知道更多的情况.

定理 4 若 $(n, 10)=1$，则 $1/n$ 的循环节长为 r，r 是满足 $10^r \equiv 1 \pmod n$ 的最小正整数.

证明 我们首先注意到，整数 r 是存在的. $1, 10, 10^2, 10^3, \cdots, 10^{n-1}$ 的最小剩余 $(\bmod n)$ 只能取值 $1, 2, 3, \cdots, n-1$，这是因为 10 的任何乘幂都不能被 n 整除. 我们又要将 n 个物体放入 $n-1$ 个盒中：必存在非负整数 a 和 b，$a \neq b$，且两数均小于 n，使 $10^a \equiv 10^b \pmod n$. 由于 $(n, 10)=1$，我们就可以用 10 的较小的那个乘幂去除此同余式的两端而得出 r.

因 $10^r \equiv 1 \pmod n$，我们知有某整数 k，使

$$10^r - 1 = kn. \tag{3}$$

以 10 为基时，k 至多有 r 位（因 $k<10^r$）. 设

$$k = d_{r-1}d_{r-2}\cdots d_1 d_0 = d_{r-1}10^{r-1} + d_{r-2}10^{r-2} + \cdots + d_1 10 + d_0,$$

其中 $0 \leqslant d_k < 10$，$k=0, 1, \cdots, r-1$. 那么由 (3) 得

[注] 实际上，当 $1/n$ 为无限循环小数时，r_i 必不能取零，故对此段证明作一补充说明，即知循环节长必不大于 $n-1$，定理也就得证. ——译校者注

$$\frac{1}{n}=\frac{k}{10^r-1}=\frac{d_{r-1}d_{r-2}\cdots d_0}{10^r}\cdot\frac{1}{1-10^{-r}}$$
$$=(.d_{r-1}d_{r-2}\cdots d_0)(1+10^{-r}+10^{-2r}+\cdots)$$
$$=.\overline{d_{r-1}d_{r-2}\cdots d_0}.$$

这就说明, $1/n$ 的循环节长至多为 r.（注意, 小数

$$.123123123123\cdots$$

也可认为是每 9 个数字重复一遍，但它的循环节长是 3.）我们还要证明, $1/n$ 的循环节长不小于 r. 假定 $1/n$ 的循环节长为 s, 且 $s<r$. 我们将表明 $10^s\equiv1(\mathrm{mod}\ n)$, 但已假定 r 是满足 $10^r\equiv1(\mathrm{mod}\ n)$ 的最小正整数, 故得矛盾. (1) 中的除法算式说明, 对任一 k, 有

$$10r_k\equiv r_{k+1}(\mathrm{mod}\ n).$$

因此,
$$10^2r_k\equiv10r_{k+1}\equiv r_{k+2}(\mathrm{mod}\ n),$$

且一般地, 对任何整数 t, 有

$$10^tr_k\equiv r_{k+t}(\mathrm{mod}\ n).$$

若 $1/n$ 的循环节长为 s, 则对所有充分大的 k, 有 $d_{k+s}=d_k$. 因而也有 $r_{k+s}=r_k$（这一结论并不是很明显的, 读者可以作出补充的说明), 也即, 对充分大的 k, 有

$$10^sr_k\equiv r_{k+s}\equiv r_k(\mathrm{mod}\ n).$$

如果我们能够证明: 对所有 k 有 $(r_k, n)=1$, 那么便可得 $10^s\equiv1(\mathrm{mod}\ n)$, 定理即可得证. 由

$$10r_{k-1}=d_kn+r_k$$

可知, 若 $p|r_k$, $p|n$, 则 $p|10r_{k-1}$. 由于 $(10, n)=1$, 故有 $p|r_{k-1}$. 同理, $p|r_{k-2}$, $\cdots$, $p|r_1$. 但由

$$10^t=d_1n+r_1,$$

我们得 $p|10$, 这不可能. 所以 $(r_k, n)=1$, 定理得证.

上述论证也可用原根的一套语言叙述出来, 而且会更优

美、更简短. 但我们没有这样做, 因为我们遵循了这样的原则: 大炮不应用来打苍蝇.

【练习 6】 应用定理 4 求 1/41 的循环节长.

遗憾的是, 还没有一般的规则可使我们一眼就看出一个整数 n 的有关数 r 是多少. 甚至使得 $r=p-1$ 的素数 p (如 7, 17, 19, 23, 29, …) 是以怎样的方式散布着, 至今人们也未能够识别出来.

以上我们只考虑了倒数, 但一般的有理数并不更为困难. 若将一个分数乘上一个并不消去它分母中的任何因子的整数, 我们不会改变它的小数展开式中的循环节长. 用一个形为 2^a5^b 的数去除一个分数时也同样如此. 因此, $1/2^a5^bn$ 与 $1/n$ 的循环节长相同; 而若 $(c, n)=1$, 则 c/n 与 $1/n$ 的循环节长也相同. 有了这些结论, 再应用定理 4, 即使对形式不是 2^a5^b 的任何 n, 我们也能求出 c/n 的小数展开式中的循环节长来.

定理 5 若 $n\neq 2^a5^b$, 且 $(c, n)=1$, 则 c/n 的小数展开式中的循环节长 r 是满足下列同余式的最小正整数:

$$10^r\equiv 1 \pmod{n},$$

其中 $n=2^a5^bn_1$, 且 $(n_1, 10)=1$.

由定理 5 和 §10 引理 1 可得, c/n 的循环节长是 $\phi(n_1)$ 的一个因子.

习 题

1. 求下列各数的小数展开式的循环节长: (a) 1/66; (b) 1/666; (c) 1/4608; (d) 1/925; (e) 1/101; (f) 1/1001.
2. 求满足 $10^r\equiv 1 \pmod{n}$ 的最小正整数 r, 其中 n 为: (a) 33; (b) 37.
3. 甲说: "我费了很大的功夫, 算出了 1/31415 的循环节长, 它正好是 15707." 乙说: "你出错了." 乙说得对不对?

4. 课文中提到，对任意非负整数 a 和 b，$1/n$ 与 $1/2^a5^bn$ 的循环节长都相同. 补上论证中略去的内容.

5. 设 $1/n$ 以 b 为基的小数展开式为

$$1/n=d_1/b+d_2/b^2+d_3/b^3+\cdots,\ 0\leqslant d_k<b.$$

证明：若此小数展开式是有限的话，则 n 的每个素因子都是 b 的一个因子.

6. 证明：若 n 的每个素因子都是 b 的一个因子，则以 b 为基时 $1/n$ 的小数展开式是有限的.

7. 以 12 为基时，13, 14, …, 25 的倒数中哪些数的小数展开式是有限的？

8. 证明：若 $(n, b)=1$，以 b 为基时，$1/n$ 的小数展开式的循环节长是满足 $b^r\equiv 1(\mathrm{mod}\ n)$ 的最小正整数.

9. 以 2 为基时，下列各数的小数展开式的循环节长是多少？(a) 1/3; (b) 1/5; (c) 1/7; (d) 1/9; (e) 1/11.

10. 以 2 为基时，求下列各数的小数展开式：(a) 1/3; (b) 1/5; (c) 1/9.

11. 以 12 为基时，下列各数的小数展开式的循环节长是多少？(a) 1/7; (b) 1/11; (c) 1/17.

12. 以 12 为基时，求下列各数的小数展开式：(a) 1/13; (b) 1/14.

13. 求下列各数的小数展开式：

(a) $1/9^2$，以 10 为基；(b) $1/7^2$，以 8 为基；

(c) $1/6^2$，以 7 为基；(d) 猜想一个定理；

(e) 证明这个定理.

14. 证明 $\sum_{n=1}^{\infty}7^{-n(n+1)/2}$ 是无理数.

§16 毕达哥拉斯三角形

3500多年前，巴比伦人就已经知道，三边分别为120，119和169的三角形是一个直角三角形．他们还知道许多其它这样的三角形，其中包括三边为下列各数的一些三角形：

$$4800,\ 4601,\ 6649;$$
$$360,\ 319,\ 481;$$
$$6480,\ 4961,\ 8161;$$
$$2400,\ 1679,\ 2929;$$
$$2700,\ 1771,\ 3229.$$

然而，这些三角形那时是派什么用处的却不清楚．本节中，我们将确定出所有这样的三角形．

著名的毕达哥拉斯定理[注]，大约是在2500年前首次得到证明的．该定理称，若x和y为一直角三角形的两直角边，z为其斜边，则

$$x^2+y^2=z^2.$$

三条边为整数的直角三角形我们称为**毕达哥拉斯三角形**．（严格说来，这些边并不是整数，而是用整数来表示其长度的一些线段.）找出所有的毕达哥拉斯三角形的问题就等同于求出下列方程的所有正整数解：

$$(1)\qquad x^2+y^2=z^2.$$

首先，我们注意到，不妨假设x与y互素．如若它们不互

［注］ 即我们通常所说的勾股定理或商高定理．——译校者注

素，即$(x, y)=d$，则因$x^2+y^2=z^2$，得$d|z$．故有

$$(x/d)^2+(y/d)^2=(z/d)^2.$$

且我们还知道，$(x/d, y/d)=1$．这就说明，欲求(1)之任意解，只要先找出使它左端两项互素的一组解，然后再乘上一个适当的因子即可．于是，要是我们求出了$x^2+y^2=z^2$的满足$(x, y)=1$的所有解，我们就能求出$x^2+y^2=z^2$的所有解．

【练习 1】 若$(x, y)=1$，且$x^2+y^2=z^2$，证明

$$(y, z)=(x, z)=1.$$

若$x=a$, $y=b$, $z=c$是$x^2+y^2=z^2$的一组解，a, b, c均为正整数，且$(a, b)=1$，我们就称这组解是一组基本解．由练习1可知，若a, b, c是一组基本解，则a, b, c中任何两个数都无大于1的公因子．

引理 1 若a, b, c为$x^2+y^2=z^2$的一组基本解，则a和b中恰有一数为偶数．

证明 在一组基本解中，整数a和b决不能同时为偶数．

【练习 2】 为什么？

a和b也不能全为奇数．假定它们全为奇数，则

$$a^2\equiv 1 \pmod 4),\ b^2\equiv 1 \pmod 4),$$

就有

$$c^2=a^2+b^2\equiv 2 \pmod 4),$$

这不可能．剩下的唯一可能性是，a和b中，一个为奇数，一个为偶数．

推论 若a, b, c是一组基本解，则c为奇数．

证明 $a^2+b^2\equiv 1 \pmod 2)$．

在我们着手为(1)的所有基本解导出一个表达式以前，我们需要证明下列引理．

引理 2 若$r^2=st$, $(s, t)=1$，则s和t均为平方数．

证明 写出s和t的素数幂分解式：

$$s=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\quad t=q_1^{f_1}q_2^{f_2}\cdots q_j^{f_j}.$$

由$(s, t)=1$，可知没有任何素数会同时出现在这两个分解式中．根据因子分解唯一性定理，r^2的素数幂分解式可写为

$$r^2=st=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}q_1^{f_1}q_2^{f_2}\cdots q_j^{f_j},$$

这些p和q是互不相同的素数．因r^2是一个平方数，所有的指数$e_1, e_2, \cdots, e_k, f_1, f_2, \cdots, f_j$就都是偶数．于是$s$和$t$就均为平方数．

【练习3】（选做） 对r用归纳法证明引理2如下：引理显然对$r=1$和$r=2$成立．假定引理对$r\leqslant n-1$成立，注意到n有一个素因子p，从而$p|s$或$p|t$，但不可能二者同时成立．另外还有$p^2|n^2$．再对n/p^2使用归纳法假设证下去．

下一引理给出了(1)的基本解必须满足的一个条件．

引理3 设a, b, c是$x^2+y^2=z^2$的一组基本解，且假定a为偶数，则存在正整数m和n，$m>n$，$(m, n)=1$，且$m\not\equiv n \pmod 2$，使

$$a=2mn,$$
$$b=m^2-n^2,$$
$$c=m^2+n^2.$$

（注意，假定a为偶数并不会失去一般性．引理1告诉我们，a和b中恰有一个偶数，故我们不妨把这对数中的偶数称作a就是了．）

证明 因a是偶数，即有某r使$a=2r$，故$a^2=4r^2$；又由$a^2=c^2-b^2$，得

$$4r^2=(c+b)(c-b). \tag{2}$$

我们知b是奇数，由引理1的推论又知c也是奇数，因此$c+b$和$c-b$均为偶数．这样，我们可令

$$c+b=2s,\quad c-b=2t. \tag{3}$$

于是，

(4) $$c=s+t,\ b=s-t.$$

将(3)代入(2)，我们得 $4r^2=(2s)(2t)$，或

$$r^2=st.$$

若 s 和 t 互素，我们就可应用引理 2 得出结论：s 和 t 均为平方数. 事实上，s 与 t 必互素，我们现在就来说明这一点. 假定 $d|s,\ d|t$，由(4)可得 $d|b,\ d|c$. 但根据练习 1，我们知 b 与 c 互素，因而 $d=\pm1$，$(s,\ t)=1$. 引理 2 说明，有某两整数 m 和 n，使

$$s=m^2,\ t=n^2,$$

且可假定 m 和 n 均为正数. 于是

$$a^2=4r^2=4st=4m^2n^2,$$

或 $a=2mn$. 由(4)得

$$c=s+t=m^2+n^2,$$
$$b=s-t=m^2-n^2.$$

求得以上三式后，我们只需再说明 $m>n$，$(m,\ n)=1$ 和 $m\not\equiv n(\mathrm{mod}\ 2)$，即可将证明完成. 由于 b 是一组基本解中的一个数，必大于零，故得 $m>n$.

【练习 4】 假定 $d|m,\ d|n$，证明 $d|a,\ d|b$，并由此推得 $(m,\ n)=1$.

【练习 5】 假定 $m\equiv n\equiv0(\mathrm{mod}\ 2)$，证明 a 和 b 均为偶数.

【练习 6】 假定 $m\equiv n\equiv1(\mathrm{mod}\ 2)$，证明 a 和 b 同样均为偶数.

练习 4、5、6 一起就可完成引理 3 的证明.

我们已经证明，若 $a,\ b,\ c$ 为一组基本解，则 $a,\ b,\ c$ 满足引理 3 的条件. 然而，如果 $a,\ b,\ c$ 满足引理 3 的条件，它们是

不是 $x^2+y^2=z^2$ 的一组基本解呢？我们在下一引理中确证这一点.

引理 4 若 $a=2mn$, $b=m^2-n^2$, $c=m^2+n^2$, 则 a, b, c 是 $x^2+y^2=z^2$ 的一组解. 如果还有 $m>n>0$, $(m, n)=1$ 和 $m\not\equiv n \pmod 2$, 则 a, b, c 就是一组基本解.

证明 欲知 a, b, c 是解, 计算一下就行了:

$$\begin{aligned} a^2+b^2 &= (2mn)^2+(m^2-n^2)^2 \\ &= 4m^2n^2+m^4-2m^2n^2+n^4=m^4+2m^2n^2+n^4 \\ &= (m^2+n^2)^2=c^2. \end{aligned}$$

余下来要证: 若 $(m, n)=1$, $m\not\equiv n \pmod 2$, 则 $(a, b)=1$. 假定 p 是一个奇素数, 满足 $p|a$ 和 $p|b$. 由 $c^2=a^2+b^2$, 知 $p|c$. 由 $p|b$ 和 $p|c$, 知 $p|(b+c)$, $p|(b-c)$. 但因

$$b+c=2m^2, \quad b-c=-2n^2,$$

故 $p|2m^2$, $p|2n^2$. 由于 p 是奇数, 故有 $p|m^2$, $p|n^2$, 因而 $p|m$, $p|n$, 但因 m 与 n 互素, 所以这是不可能的. a 与 b 不互素还有一种可能的情况, 即它们都能被 2 整除. 但因 $b=m^2-n^2$, 且 m 和 n 两数中, 一个是偶数, 一个是奇数, 所以 b 是奇数. 于是 $(a, b)=1$. 又因 $m>n$, 故 b 是正数; 由于 m 和 n 是正数, 故 a 也是正数. 于是 a, b, c 是一组基本解.

我们将引理 3 和引理 4 重新叙述为

定理 1 $x^2+y^2=z^2$ 的所有解 $x=a$, $y=b$, $z=c$ (其中 a, b, c 全为正数且无大于 1 的公因子, a 为偶数) 均可写为

$$\begin{aligned} a &= 2mn \\ b &= m^2-n^2 \\ c &= m^2+n^2 \end{aligned}$$

其中 m 和 n 是互素的整数且不同为奇数, $m>n$.

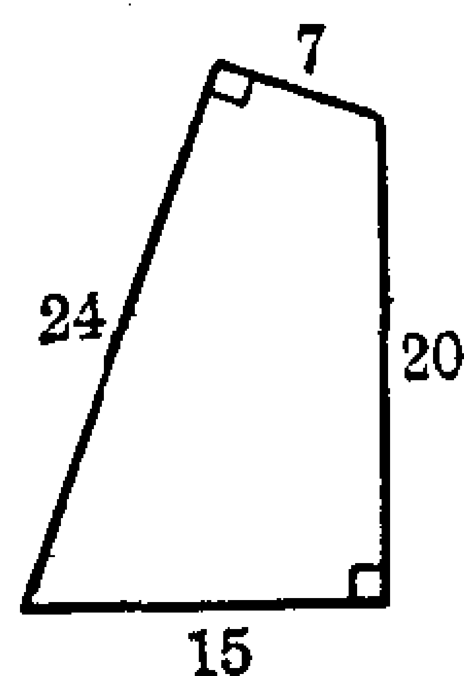
下表列出了一些有关数字较小的基本的毕达哥拉斯三角形：

m	n	a	b	c	a^2	b^2	c^2
2	1	4	3	5	16	9	25
3	2	12	5	13	144	25	169
4	1	8	15	17	64	225	289
4	3	24	7	25	576	49	625
5	2	20	21	29	400	441	841
5	4	40	9	41	1600	81	1681
6	1	12	35	37	144	1225	1369
7	2	28	45	53	784	2025	2809

习　题

1. 除了上表中已列出的以外，还有多少个毕达哥拉斯三角形其斜边小于50？
2. 找出一个各边均大于50的毕达哥拉斯三角形．
3. 若$(a, b)=d$, $a^2+b^2=c^2$, 证明$(a, c)=(b, c)=d$.
4. (a) 若a, b, c是根据定理1由m和n产生的，证明
$$(b+c)/a=m/n;$$
(b) 什么样的m和n可得出$72^2+65^2=97^2$？
5. 若$(a, b)=1$, $ab=c^n$，能不能得出a和b都是n次方数？
6. 证明：若相继的两个整数的和是一个平方数，则较小的那个数是一个毕达哥拉斯三角形的一条直角边，较大的那个数是它的斜边．
7. 巴斯喀拉(Bhascara, 1150年左右)曾作出一个直角三角形，它的面积在数值上等于它的斜边长．证明边长为整数的三角形不可能发生这一情况．
8. 课文中列出的表上，所有毕达哥拉斯三角形都有一条边是5的倍数，是否所有毕达哥拉斯三角形都是如此呢？
9. 证明12整除任一毕达哥拉斯三角形两直角边的乘积．
10. 证明60整除任一毕达哥拉斯三角形各边的乘积．

11. 这里有一个四边形，它不是平行四边形，其各边和面积均是整数:



(a) 它的面积是多少？

(b) 你能找出另一个这样的四边形吗？

(c) 你能再找出1,000,000个这样的四边形来吗？

12. 设一个毕达哥拉斯三角形由相继的两个三角形数(按基本解的公式)产生，证明这个三角形必有一边是一个立方数.

13. 3, 4, 5是$x^2+y^2=z^2$的一组具有相继的三个正整数的解，证明这样的解是唯一的.

14. 证明：三边成算术级数的毕达哥拉斯三角形就是以$3n$, $4n$, $5n$ ($n=1, 2, 3, \cdots$)为三边构成的三角形.

15. $3^2+4^2=5^2$, $5^2+12^2=13^2$, $7^2+24^2=25^2$, $9^2+40^2=41^2$.

(a) 猜想一个定理;

(b) 证明(a)中提出的那些数给出了一条直角边和斜边为相继的整数的所有毕达哥拉斯三角形.

16. (a) 查看一下课文列出的表，找出具有相同面积的两个毕达哥拉斯三角形;

(b) 你能找到另外两个面积相同的毕达哥拉斯三角形吗？

(c) 证明：面积和斜边分别相等的两个毕达哥拉斯三角形全等.

17. 证明$n^2+(n+1)^2=2m^2$不可能成立.

18. 证明：只有当-1是一个二次剩余(mod k)时，才有可能成立

$$n^2+(n+1)^2=km^2.$$

19. 注意，$4^2-3^2=7$, $12^2-5^2=7\cdot17$, $8^2-15^2=-7\cdot23$. 证明：若$a^2+b^2=c^2$，且$(7, abc)=1$，则$7|(a^2-b^2)$.

20. 虽然9不是两个正整数的平方和，但它是两个正有理数的平方和，求出这两个正有理数.

21. (a) 给定a，怎样求出b使a^2+b^2是一个平方数？

(b) 对$a=13$和$a=14$，用你在(a)中得出的方法求出b.

22. 求一个毕达哥拉斯三角形，它的面积在数值上等于它的周长.

23. (a) $3^2+4^2=5^2$, $20^2+21^2=29^2$, $119^2+120^2=169^2$. 为了求得另

一个这样的关系式，证明：若 $a^2+(a+1)^2=c^2$，则

$$(3a+2c+1)^2+(3a+2c+2)^2=(4a+3c+2)^2;$$

(b) 给出如(a)所述的另一个数值例子；

(c) 若 $a^2+(a+1)^2=c^2$，且令 $u=c-a-1$，$v=(2a+1-c)/2$，证明 v 是一个整数，且 $u(u+1)/2=v^2$.（这就表明，有无限多个三角形数同时也为平方数.）

§17 无限递降法和费马猜想

在毕达哥拉斯三角形一节中，我们求得了 $x^2+y^2=z^2$ 的所有整数解．处理了这个问题后，很自然地就想用同样的想法来试一试方程 $x^3+y^3=z^3$，它的次数比上节考虑的方程增加了1．然而，同样的想法失效了，而且其它别的想法也无济于事，因为 $x^3+y^3=z^3$ 就根本无解．（只有一个例外，即变数之一取零时，会有整数解，我们把这样的解称为平凡解，并认为这种解不值得我们多费笔墨．本节中我们所说的"解"是指"非平凡解"．）事实上，对于 $n\geqslant 3$ 的任一方程 $x^n+y^n=z^n$，谁也没有找到整数解．费马曾认为他已能证明，当 $n\geqslant 3$ 时，$x^n+y^n=z^n$ 都没有非平凡解．他在丢番图的一本著作上作出的一个傍注中写道，他已有一个证明，但地方太小写不下．我们几乎可以肯定他是弄错了．当然，我们也不能完全肯定是这样，他也许真的找到了一个证明，而且，他也许已经意识到，这一证明非常深奥，因而写下了上述批注，好让未来的数学家们多动动脑筋．

"当 $n\geqslant 3$ 时，$x^n+y^n=z^n$ 没有非平凡解"这一论断常被称作"费马大定理"，以便与也是用他的名字命名的那个定理（见§6）区分开来；然而，"费马猜想"应是一个更为合适的名称．已有大量的著作专门论述这一问题，但是仍然没有哪一种方法能使它得到解决．已经知道，对于小于25,000的 n 值以及许多更大的 n 值，费马猜想是成立的，但这些结果离开这个猜想的证明仍很遥远．在第一次世界大战以前，德国曾经设置

了一笔很大的奖金，征求正确的证明．许多业余爱好者进行了尝试，并寄去了自己的解答．据说，著名的数论专家朗道(Landau)请人印了许多明信片，上面写道："亲爱的先生或女士：你对费马的定理的证明已经收到，现予退回．第一个错误出现在第____页第____行．"朗道将这些明信片分发给他的学生们，吩咐他们将相应的数字填上去．许多很有能力的数学家都曾研究过费马猜想的问题．由于 $x^n+y^n=z^n$ 可能存在着一组解，但其数字实在太大了，以致没有人能够把它们求出来，因此可能永远不会有哪种方法可以判定费马猜想是否成立．

本节的论题是要证明 $n=4$ 时费马猜想是成立的，并借此介绍费马的无限递降法．（你可能会感到纳闷，我们为什么要避开 $n=3$ 这一情况呢？原来，人们发现，虽然无限递降法也适用于 $n=3$ 的情况，但要证明 $x^3+y^3=z^3$ 无解要比证明 $x^4+y^4=z^4$ 无解更为困难．对 $n=3$ 的情况，读者可参考有关书刊．）我们来证明

定理 1 下列方程没有非平凡解：

$$x^4+y^4=z^2.$$

注意，这也意味着，$x^4+y^4=z^4$ 无解，因为若 a, b, c 是此方程的解，则有 $a^4+b^4=(c^2)^2$，与定理 1 矛盾．

定理 1 的证明 我们将使用费马的无限递降法．考虑 $x^4+y^4=z^2$ 的所有非平凡解的集合，我们要证明这个集合是空集．假定它不是空集，我们将推出矛盾．在这个非平凡解的集合中，必有一组解使 z^2 的值最小，设 c^2 就是 z^2 的这个值．使 z 取此值的解可能有好几组，要是那样的话，我们可取任一组解（取哪一组解都一样），并将它记作 a, b, c．证明的思想是：造出一组数 r, s, t，使它们也满足 $x^4+y^4=z^2$，但 $t^2<c^2$.

鉴于 c^2 已被选得尽可能地小，因而知解集非空的假定是错误的，故该方程没有非平凡解. 这一方法决不单单是一种技巧，而是一件相当自然的事. 情况很可能是这样的：有一次，费马着手寻求 $x^4+y^4=z^4$ 的解，他可能千方百计地应用了我们以前对方程 $x^2+y^2=z^2$ 进行化约的方法，以化约上述方程. 当他看到自己努力的结果是得到了形式相同的方程和数值较小的解，他也许感到有点惊奇，也可说是感到惊喜，因为这使他能得出结论：若此方程有解，即可找出另一个数值较小的解，然后又可找出另一个，如此一个一个找下去，即得一串无限下降的解，但由于我们可以假定 x, y, z 都为正数，因而这是不可能的. （与此同时，也许费马坐了下来，心想："我现在要对 $x^4+y^4=z^4$ 应用我这个无限递降法"，但对这个问题历史却没有提供任何材料.）

我们假定，已有一组非平凡解 a, b, c，而 c^2 是可能取到的值中的最小值，我们还可认为 a 和 b 互素. 要是它们不互素，就有一个素数 p 使 $p|a$, $p|b$，从而 $p^2|c$. 于是，$(a/p)^4+(b/p)^4=(c/p^2)^2$，它为 $x^4+y^4=z^2$ 提供了另一组解，且相应的 z^2 的值比 c^2 还要小，但我们已经假定这是不可能的.

【练习 1】 证明 a 和 b 不能同为奇数. （对模 4 考虑 $a^4+b^4=c^2$.）

由于 $(a, b)=1$，a 和 b 也不能同为偶数. 因此，它们中一个为偶数，一个为奇数. 由于 $a^4+b^4=c^2$ 关于 a 和 b 是对称的，我们可约定将这对数中的偶数记作 a. 现在我们对 $x^2+y^2=z^2$ 有了一组在上节加以定义的基本解：

$$(a^2)^2+(b^2)^2=c^2,$$

其中，$(a^2, b^2)=1$，a^2 为偶数，b^2 为奇数. 因此，由上节引理 3 知，存在整数 m 和 n，两数互素，且不同为奇数，使

$$(1)\qquad \begin{cases} a^2=2mn, \\ b^2=m^2-n^2, \\ c=m^2+n^2. \end{cases}$$

【练习 2】 证明 n 是偶数. (假定 n 为奇数, m 为偶数, 用模 4 考察 $b^2=m^2-n^2$. 记住: $x^2\equiv -1 \pmod 4$ 是不可能的.)

由于 n 是偶数, 可知 m 是奇数. 令 $n=2q$, 那么由 (1) 得 $a^2=4mq$, 或

$$(2)\qquad \left(\frac{a}{2}\right)^2=mq.$$

我们要推证, m 和 q 均为平方数. 为此, 根据上节引理 2, 我们需证 m 与 q 互素.

【练习 3】 证明 $(m, q)=1$. (要是它们不互素, 则 $(m, n)\neq 1$.)

因此, 存在整数 t 和 v, 使

$$m=t^2,\quad q=v^2.$$

【练习 4】 验证 t 和 v 互素. (要是不互素的话, 则有 $(m, q)\neq 1$.)

【练习 5】 说明 t 是奇数. (否则, m 就是偶数.)

到此为止, 关于 a, b, c, 我们已经知道了许多事情, 但还需要更多的情况. 首先, 我们容易看到

$$n^2+(m^2-n^2)=m^2.$$

又我们已知有下列各式:

$$n=2q=2v^2,\quad m^2-n^2=b^2,\quad m=t^2,$$

将它们代入前式, 就有

$$(2v^2)^2+b^2=(t^2)^2,$$

我们求得了另一个毕达哥拉斯三角形. $2v^2$, b, t^2 是一组基

本解吗？如果 $2v^2$ 与 b 互素，它们就是一组基本解，我们在以下练习中即会发现这一点.

【练习 6】 说明为什么下列几个结论成立:

(a) 若 $p|2v^2$, $p|b$, 则 $p|n$, $p|b$;

(b) 若 $p|n$, $p|b$, 则 $p|n$, $p|m$;

(c) 若 $(m, n)=1$, 则 $(2v^2, b)=1$.

于是，我们又得到了 $x^2+y^2=z^2$ 的一组基本解，其中 $2v^2$ 是偶数. 从而我们只需利用上节引理 3 就可知道，存在整数 M 和 N，其中 $(M, N)=1$, $M\not\equiv N \pmod 2$，使

$$(3)\qquad \begin{cases} 2v^2=2MN, \\ b=M^2-N^2, \\ t^2=M^2+N^2. \end{cases}$$

因此我们有 $v^2=MN$, $(M, N)=1$. 两个互素的整数，当且仅当它们都是平方数时，它们的乘积也是平方数（上节引理 2）. 所以，存在整数 r 和 s, 使

$$M=r^2, \quad N=s^2.$$

由 (3) 之第三式，我们得

$$t^2=(r^2)^2+(s^2)^2,$$

或

$$r^4+s^4=t^2,$$

这就得出了 $x^4+y^4=z^2$ 的另一组解，而这组解具有下列性质:

$$t^2=m\leqslant m^2<m^2+n^2=c\leqslant c^2,$$

这是不可能的，因为 c^2 是最小的所能选取的数. 这一矛盾使定理得证.

【练习 7】 为什么 $m^2<m^2+n^2$，而不是 $m^2\leqslant m^2+n^2$?

下面是无限递降法的另一例子，它略有不同之处，且远没有定理 1 那样重要. 假定我们欲求整数 a, b, c, 使

$$\begin{vmatrix} 1 & a & b \\ a & 1 & c \\ b & c & 1 \end{vmatrix} = 1.$$

若我们将此行列式展开，这就无异于要求整数 a, b, c, 使它们满足

(4) $$x^2+y^2+z^2=2xyz.$$

【练习 8】 证明：a, b, c 不可能全为奇数，也不可能两个是偶数而第三个是奇数.

它们中也不可能两个为奇数而第三个为偶数. (要是可能的话，对(4)取模 4，就会有 $2\equiv 0 \pmod 4$.) 因此，若 a, b, c 满足(4)，它们必全为偶数，而 $a/2$, $b/2$, $c/2$ 就都是整数. 用 4 除(4)，得

(5) $$(a/2)^2+(b/2)^2+(c/2)^2=4(a/2)(b/2)(c/2).$$

说明 a, b, c 全为偶数而用到的上述论证方法也可用来证明 $a/2$, $b/2$, $c/2$ 全为偶数. 因此 $a/4$, $b/4$, $c/4$ 就都是整数. 用 4 除(5)，就有

$$(a/4)^2+(b/4)^2+(c/4)^2=8(a/4)(b/4)(c/4).$$

再用同样的论证方法即可说明，$a/8$, $b/8$, $c/8$ 全为整数. 如此继续下去，我们发现，对一切正整数 n, $a/2^n$, $b/2^n$, $c/2^n$ 都是整数. 而满足这一条件的整数只有 $a=b=c=0$，它们就是(4)的唯一的一组解.

习　题

1. 证明：$x^{4n}+y^{4n}=z^{4n}$, $n=1, 2, \cdots$, 没有非平凡解.
2. 假定我们可以证明：对任一奇素数 p, $x^p+y^p=z^p$ 没有非平凡解. 根据这个假定和习题 1 的结果推证：对于任何 $n\geqslant 3$, $x^n+y^n=z^n$ 没有非平凡解.

3. 证明：由 $x^p+y^p=z^p$ 可得 $p|(x+y-z)$.
4. 证明：除非 $p|xyz$，否则 $x^{p-1}+y^{p-1}=z^{p-1}$ 没有非平凡解.
5. $x^2+(x+2)^2=y^2$ 有没有基本解？
6. 考虑 $x^2+y^2+z^2=kxyz$. 当 k 为哪些值时，利用课文中提出的论证方法可以证明 $x=y=z=0$ 是此方程的唯一解？
7. 证明下列方程没有非平凡解：

   (a) $x^2+y^2=x^2y^2$; (b) $x^2+y^2+z^2=x^2y^2$.
8. 证明：对于任何 $n\geqslant 1$,

$$x^n+y^n=z^{n+1}$$

具有无限多组非平凡解，它们是

$$x=(ac)^{rn},\ y=(bc)^{rn},\ z=c^s,$$

其中 $c=a^{rn^2}+b^{rn^2}$，a 和 b 可为任意整数，而 r 和 s 的选取应使其满足

$$rn^2+1=(n+1)s.$$

最后一个方程关于 r 和 s 有无限多组正整数解吗？

9. 求出 $x^4+y^4=z^5$ 的一组解.
10. 证明：对于任何正整数 n，$x^n+y^n=z^n$ 都不存在 x 和 y 均小于 n 的解.
11. 找下列方程的解：$x^n+y^n=z^{n-1}$.
12. 证明：若 $(n,\ m)=1$，$x^n+y^n=z^m$ 必有非平凡解.

§18　两个平方数的和

从1到99的整数中，下列57个不能表为两个整数的平方和：

3　6　7　11　12　14　15　19　21　22　23　24
27　28　30　31　33　35　38　39　42　43　44　46
47　48　51　54　55　56　57　59　60　62　63　66
67　69　70　71　75　76　77　78　79　83　84　86
87　88　91　92　93　94　95　96　99.

但其余42个都可以表为两个整数的平方和：

1　2　4　5　8　9　10　13　16　17　18　20
25　26　29　32　34　36　37　40　41　45　49　50
52　53　58　61　64　65　68　72　73　74　80　81
82　85　89　90　97　98.

如果你考察一下这两张表，并试一试用科学的方法提出一条假设，以说明一个数在什么情况下会出现在哪一张表上，并借此预计大于99的数的有关结果，那么，这对你的归纳能力将是一种良好的训练. 在第一张表中，各数有着一个相当简单的共同特征（并非指它们不能表为两个平方数之和这一点），我们可证明下列引理，以帮助我们在正确的方向上努力.

引理1　若$n\equiv3 \pmod 4$，则$n=x^2+y^2$是不可能的.

证明　由于对一切整数x，有$x^2\equiv0$或$1 \pmod 4$，所以对任何x和y，有

$$x^2+y^2\equiv 0,\ 1 \text{ 或 } 2\ (\bmod 4),$$

故 $x^2+y^2\equiv 3(\bmod 4)$是不可能的. 这一引理解释了第一张表的 57 个数中的 25 个为什么出现在这张表上.

引理 2 若 n 是可表示的, 则对任一 k, k^2n 也是可表示的. (有时我们将 "n 可表示为两个平方数之和" 简单地说成 "n 是可表示的".)

证明 若 $n=x^2+y^2$, 则 $k^2n=(kx)^2+(ky)^2$.

如果你放弃了自己的努力, 那么下面就有这个问题的答案:

定理 1 n 不能表示为两个平方数之和的充要条件是: n 的素数幂分解式中有一个素因子与 3 同余$(\bmod 4)$, 且它的幂次为奇数.

证明(充分性部分) 假定 p 为素数, $p\equiv 3(\bmod 4)$, 且它以奇次幂出现在 n 的素数幂分解式中, 即对某一 e 有, $p^{2e+1}|n$, 但 $p^{2e+2}\nmid n$. 假定对某 x 和 y, 有 $n=x^2+y^2$, 我们将推出 -1 是一个二次剩余 $(\bmod p)$, 但因 $p\equiv 3(\bmod 4)$, 故这一结论是不可能的, 于是便得出矛盾. 设 $d=(x, y)$, $x_1=x/d$, $y_1=y/d$, $n_1=n/d^2$, 那么,

(1) $$x_1^2+y_1^2=n_1, \text{ 其中, } (x_1,\ y_1)=1.$$

如 p^f 是整除 d 的 p 的最高次幂, 则 n_1 可被 $p^{2e-2f+1}$ 整除, 且因这一指数是非负奇数, 故至少为 1, 因而 $p|n_1$. 又由于 $(x_1,\ y_1)=1$, 我们有 $p\nmid x_1$, 从而有一个数 u 使

$$x_1u\equiv y_1(\bmod p).$$

于是,

(2) $$0\equiv n_1\equiv x_1^2+y_1^2\equiv x_1^2+(ux_1)^2\equiv x_1^2(1+u^2)\ (\bmod p).$$

由于$(x_1,\ p)=1$, 在(2)中可消去 x_1, 得

$$1+u^2\equiv 0(\bmod p).$$

这就说明，-1 是一个二次剩余$(\bmod p)$，而这是不可能的. 因此，$n=x^2+y^2$ 不可能成立，我们就证明了定理中较为容易的一部分.

本节以下内容全用来证明定理1的必要性部分. 我们需要两个引理.

引理3 对任意整数 a, b, c, d, 有

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2.$$

证明 相乘展开即知.

这一结果表明，若两个数是可表示的，则它们的乘积也是可表示的.

引理4 任一整数均可写为

$$n=k^2p_1p_2\cdots p_r,$$

其中 k 是一个整数，各个 p_i 是互不相同的素数.

【练习1】 考虑 n 的素数幂分解式，进而说明上述结论是正确的.

现举一例来应用引理2和引理3. 根据表示式 $5=2^2+1^2$ 和 $13=3^2+2^2$，我们来求 $260=2^2\cdot5\cdot13$ 的一个表示式. 由引理3,

$$65=5\cdot13=(2^2+1^2)(3^2+2^2)$$
$$=(2\cdot3+1\cdot2)^2+(2\cdot2-1\cdot3)^2=8^2+1^2$$

所以，$260=2^2\cdot65=(8\cdot2)^2+(1\cdot2)^2=16^2+2^2.$

【练习2】 将325写成两个平方数的和.

【练习3】 如果 n 的素数幂分解式中不包含满足 $p\equiv3\ (\bmod 4)$ 且幂次为奇数的素因子 p，那么对某 k 和 r，有

$$n=k^2p_1p_2\cdots p_r \quad 或 \quad n=2k^2p_1p_2\cdots p_r,$$

其中每个 p_i 都与1同余$(\bmod 4)$. 说明这一结论.

练习3、引理2和引理3说明了，要证明定理1的必要性

部分，我们只需证明

定理 2 每个与 1 同余 (mod 4) 的素数均可写为两个平方数之和.

证明 证明的思想是这样的：若 $p\equiv 1(\bmod 4)$，则我们可先说明，存在着非零的整数 x 和 y，使

$$x^2+y^2=kp,$$

k 为某一整数，且 $k\geqslant 1$；然后再证明，若 $k>1$，我们就可由 x 和 y 造出新的整数 x_1 和 y_1，使

$$x_1^2+y_1^2=k_1p,$$

且 $k_1<k$. 有了这一步，定理 2 就能得证，这是因为，若 $k_1>1$，我们可重复上述步骤而得 x_2 和 y_2，使 $x_2^2+y_2^2=k_2p$，且 $k_2<k_1$. 如此继续下去，我们就会求得一递减的正整数列，它的各个元素满足 $k>k_1>k_2>\cdots$，最后必得一个元素为 1，此时我们就已将 p 表为两个平方数的和了.

我们首先证明，可以求得非零的 x 和 y，使对某 k，$k\geqslant 1$，有 $x^2+y^2=kp$. 由于 $p\equiv 1(\bmod 4)$，我们知，-1 是一个二次剩余 $(\bmod p)$，故存在一个整数 u，使 $u^2\equiv -1(\bmod p)$，即 $p\mid(u^2+1)$. 故对某 k，$k\geqslant 1$，有

$$u^2+1=kp,$$

也即对某 k，$k\geqslant 1$，$x^2+y^2=kp$ 总有一解. 事实上，我们可设 $y=1$. 例如，若 $p=17$，我们有 $4^2+1^2=1\cdot 17$；若 $p=29$，则有 $12^2+1^2=5\cdot 29$. 数 u 可用尝试法求出（我们可对 $k=1, 2, \cdots$ 依次写下 $kp-1$，直到求得一个平方数为止），也可利用下式求出 u：

$$\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv -1(\bmod p).$$

这一同余式（它可由威尔逊定理得出）给出了 u 的构造方法.

此法可能很繁，但总能保证求得结果.

现在我们来说明如何造出 x_1 和 y_1. 定义 r 和 s 如下:

(3) $$r\equiv x(\mathrm{mod}\ k),\ s\equiv y(\mathrm{mod}\ k),$$

其中，$-\frac{k}{2}<r\leqslant\frac{k}{2}$，$-\frac{k}{2}<s\leqslant\frac{k}{2}$. 由(3)可得

$$r^2+s^2\equiv x^2+y^2(\mathrm{mod}\ k).$$

但我们已经选取 x 和 y，使 $x^2+y^2=kp$，因而

$$r^2+s^2\equiv 0(\mathrm{mod}\ k),$$

即对某 k_1，有

(4) $$r^2+s^2=k_1k.$$

由(4)得 $$(r^2+s^2)(x^2+y^2)=(k_1k)(kp)=k_1k^2p.$$

而由引理 3，我们有

$$(r^2+s^2)(x^2+y^2)=(rx+sy)^2+(ry-sx)^2.$$

因此，

(5) $$(rx+sy)^2+(ry-sx)^2=k_1k^2p.$$

由(3)还可注意到

$$rx+sy\equiv r^2+s^2\equiv 0(\mathrm{mod}\ k),$$
$$ry-sx\equiv rs-sr\equiv 0(\mathrm{mod}\ k),$$

因此，k^2 整除(5)之左端各项. 将(5)式除以 k^2，便得下列方程:

$$\left(\frac{rx+sy}{k}\right)^2+\left(\frac{ry-sx}{k}\right)^2=k_1p,$$

其中有关数均为整数. 可令 $x_1=(rx+sy)/k$, $y_1=(ry-sx)/k$，则 $x_1^2+y_1^2=k_1p$. 如我们能证 $k_1<k$，定理也就得证. 由(3)中之不等式条件可知

$$r^2+s^2\leqslant(k/2)^2+(k/2)^2=k^2/2.$$

但因 $$r^2+s^2=k_1k,$$

所以，$k_1k\leqslant k^2/2$，从而 $k_1\leqslant k/2$. 故有 $k_1<k$，定理得证. (注

意，$k_1\geqslant 1$，因为如 $k_1=0$，则由上式，$r=s=0$，这是不可能的.）[注]

【练习 4】 在上述证明中，为什么 $r=s=0$ 是不可能的？

让我们举一个例子. 我们从 $12^2+1^2=5\cdot 29$ 开始，进行定理所要求的全部演算，以求得 29 写为两平方数之和的表示式. 可取 $x=12, y=1$，$k=5$. 于是有 $r\equiv 12 \pmod 5$，$s\equiv 1 \pmod 5$；在适当范围内选取 r 和 s，可得 $r=2$，$s=1$. 因此，

$$\begin{aligned}5^2\cdot 29&=(2^2+1^2)(12^2+1^2)\\&=(2\cdot 12+1\cdot 1)^2+(2\cdot 1-1\cdot 12)^2\\&=25^2+10^2.\end{aligned}$$

用 $k^2=25$ 相除，得 $29=5^2+2^2$，这就是欲求之表示式.

【练习 5】 试对 $23^2+1^2=10\cdot 53$ 进行上述演算.

结束本节前，我们要对与两个平方数之和的问题密切相关的丢番图方程（即不定方程）说几句话. 我们已经完全解决了将一个整数表为两个平方数之和的问题：我们知道到底有哪些整数可这样表示，而定理 2 及其前面几个引理还给出了实际求出这种表示式的方法. 现在，很自然地想要了解将一个整数表为三个平方数之和的问题. 可以预料，多加一个平方数，就会有更多的整数可以表示，情况也的确如此. 事实上，除了 $n=4^e(8k+7)$（其中 e 和 k 均为整数）以外，其它 n 均可写为三个平方数之和. 100 以内不能写为三个平方数之和的数为

[注] 以上证明中，虽有 $k_1\geqslant 1$，但却不能保证 k_2，k_3，等等都 $\geqslant 1$. 例如，设 $p=5$，可取 $x=y=5$，$k=10$. 用上法递推可知，$k_1=5$，$k_2=0$. 这一情况是与没有要求 $k<p$ 有联系的. 事实上，我们可证：总能求得非零的 x，y 和 k，使 $x^2+y^2=kp$，且 $1\leqslant k<p$. 再对此 k 进行递推，即可保证以后各个 k_i 均 $\geqslant 1$. ——译校者注

7, 15, 23, 28, 31, 39, 47, 55, 60, 63,

71, 79, 87, 92, 95.

它们共有 15 个，而只允许写成两个平方数之和时，却有 57 个不能表示．若我们考虑四个平方数之和的问题，例外情况甚至会更少，实际上根本就没有．在下节中我们就要表明，每个整数都可写为四个平方数之和．

看来平方数问题算是解决了（仅就能否表示而言，当然还有许许多多其它问题可以追问，且其中有些问题已能解答．例如，一个整数写成两个平方数之和，其表示式可有多少种？当 $n=1, 2, \cdots, N$ 时，$x^2+y^2=n^2$ 有多少组解？如此等等．一个问题刚得到解决，大量其它的问题又代之而起．）立方数问题怎么样？的确，每个整数都可写为九个立方数之和，但谁都不清楚四次方数之和的相应数目是多少（虽然已经知道，任一大于 $10^{10^{89}}$ 的整数均可表为 19 个四次方数之和），也不知道需要多少个五次方数来表示每一个数．但对六次方数、七次方数以及几乎所有更高次方的数，答案倒已得出．例如，六次方数需要 73 个．设 $g(k)$ 是使每个整数可以写为不超过 s 个 k 次方数之和的最小 s 值，求 $g(k)$ 的问题称为华林问题．1770 年，华林（Waring）曾经写道，每一整数是 4 个平方数之和，9 个立方数之和，19 个四次方数之和，等等．但这仅是他的猜想而已；直到 1909 年，才有人证明：对每个 k，都存在着 $g(k)$．然而，当 k 较大时，$g(k)$ 到底有多大？甚至到那时也仍几乎一无所知．后来的研究表明，对于 $6\leqslant k\leqslant 20,000$ 及一切“充分大”的 k，$g(k)=2^k+[(3/2)^k]-2$；而对所有 $k\geqslant 6$，这一公式是否成立？许多人是非常怀疑的．（记号 $[(3/2)^k]$ 表示 $(3/2)^k$ 的整数部分，见附录二．）比 $g(k)$ 更有意思的是 $G(k)$，它是使每一“充分大”的整数能写出不超过 s 个 k 次方数之和的最小

s 值．$G(2)=4$，$G(4)=16$，但当 k 为更大的值时 G 到底多大却不清楚．对于一般情况知道的最好结论是

$$k+1\leqslant G(k)\leqslant k(3\log k+11)$$

右边这一不等式证明起来极为困难和复杂，这一成就是维诺格拉多夫（Vinogradov）在哈代（Hardy）和李特尔沃特（Littlewood）所得结果的基础上取得的，它代表了数论的高峰之一．

将整数表为另外一些整数之和的另一著名问题是哥德巴赫猜想．1742 年，哥德巴赫（Goldbach）注意到

$$4=2+2,\quad 6=3+3,\quad 8=5+3,\quad 10=5+5,$$
$$12=7+5,\quad 14=7+7,\quad \cdots,\quad 100=97+3,$$

他猜想，每一大于 2 的偶数均可表为两个素数之和．他问欧拉能否证明，欧拉失败了，而且至今未有人取得成功．我们能说的，充其量不过是：每一大于 2 的偶数可以写为不超过 $2\cdot10^{10}$ 个素数之和[注1]．维诺格拉多夫用种种不同的方法证得，每个"充分大"的偶数是不多于 4 个素数的和．后来又有人证明了，"充分大"三字可用"大于 $e^{e^{16.038}}$"来代替．（这里，e 不代表一个整数，而是自然对数的底：$e=2.718\cdots$．）在另一方向上，有人在 1966 年宣布[注2]，每一充分大的偶数是一个素数和另一整数之和，而此整数的不同的素因子数不超过 2．这是最为接近解决这一猜想的结果了．

［注 1］ 近年来，有人已能证明，任何大于或等于 2 的整数可以表示为不超过 27 个素数之和．（参见王元"谈谈素数"一书的介绍第 56 页，1978 年 11 月上海教育出版社出版．）——译校者注

［注 2］ 指我国数学家陈景润于 1966 年 5 月在"科学通报"第 17 卷第 19 期上发表的著名结果："每一个充分大的偶数都能够表示为一个素数及一个不超过 2 个素数的乘积之和．"1973 年"中国科学"第 2 期刊登了这一结果的详细证明．——译校者注

习　题

1. 判断下列整数中哪些可以写为两个平方数之和，并对可以表示的哪些数，各求出一个表示式：150, 151, 152, 153, 154.
2. 1965, 1966, 1967, 1968, 1969, 1970 这几个数中，哪些能写为两个平方数之和？
3. 将 10045, 10048, 10049 分别表示为两个平方数的和.
4. 不引用定理 1 直接证明：若 $7|n$, $7^2\nmid n$, 则 $n=x^2+y^2$ 是不可能的
5. 证明：若 $n\equiv 3$ 或 $6 \pmod 9$, 则 n 不能表为两个平方数之和.
6. "若 $5|n$, $5^2\nmid n$, 则 $n=x^2+y^2$ 是不可能的."这一说法正确吗？
7. 证明：若 m 和 n 都是两个平方数的和，且 $m|n$, 则 n/m 也是两个平方数的和.
8. 费马说："$2n+1$ 是两个平方数之和的充分必要条件为：(i) n 为偶数，(ii) $2n+1$ 除以它最大的平方数因子后所得之数不能被一个素数 $4k-1$ 整除."证明这一说法与定理 1 等价.
9. 吉兰德(Girard, 1632 年)曾说过，能表为两个平方数之和的数由下列一些数构成：所有平方数、所有形为 $4k+1$ 的素数、这些数的乘积以及前面这些数中任一数的 2 倍. 证明这一说法和定理 1 等价.
10. 在 $100\leqslant n\leqslant 150$ 这一范围内的哪些整数可以写为三个平方数的和？
11. 证明：由 $4|(x^2+y^2+z^2)$ 可知 x, y, z 均为偶数.
12. 证明：若 $n\equiv 7 \pmod 8$, 则 n 不能写为三个平方数之和.
13. 根据题 11 和题 12 的结果，证明：若对某两个非负数 e 和 k, 有 $n=4^e(8k+7)$, 则 $n=x^2+y^2+z^2$ 是不可能的.
14. 一位数学家在 1621 年说，若对某 k, 有 $n=8k+2$ 或 $n=32k+9$, 则 $3n+1$ 不是三个平方数之和. 这个结论正确吗？
15. 模仿定理 2 的证明，试试看能否得到一个推广：若 $(-w/p)=1$, 则存在整数 x 和 y 使 $p=x^2+wy^2$.
16. 证明：若 n 是两个三角形数之和，则 $4n+1$ 是两个平方数之和.
17. 哪些整数可以写为两个有理数的平方和？

§19 四个平方数的和

我们将要在本节中证明，每一正整数均可写为四个整数的平方和(其中有些整数可以为零)．这一定理的历史相当悠久．丢番图就似乎已经认为，每一正整数都是两个、三个或四个正整数的平方和，不过他从未将此作为定理明确叙述出来．第一个做这件事的人是巴契特(Bachet, 1621年)，他从1起，一直验证到325，都说明这是正确的，但他无法证明这个定理．费马说，他能够用他的递降法作出证明，然而照例他又未提供任何细节．从他后来关于这一定理的著作来看，他的证明是否完整，这是值得怀疑的．笛卡儿也说过这一定理无疑是正确的，但他认为要找出证明“实在太难了，以至我不敢动手去找”．

下一个接受挑战的是欧拉，他在1730年首次开始研究这一问题．1743年，他注意到，两个四平方数之和的乘积仍为四平方数之和，这一结果对于上面定理的证明非常重要，事实上，他差“一点”就证明了这个定理．1751年，他仍在研究着那个“一点”的时候，证得了另一个基本的结果，即：$1+x^2+y^2\equiv 0(\bmod p)$($p$为任一素数)总有一解．但是，他仍未能把定理证出．直到1770年，拉格朗日才成功地作出了一个证明，他在很大程度上依据的就是欧拉的思想．1773年，欧拉(那时已经66岁)给出了一个更为简单的证明，也就是说，欧拉取得这一成就，一共经过了43年！

我们首先证明欧拉的两个结果．

引理 1 两个四平方数之和的乘积仍是四平方数之和.

证明 证明极其浅显. 不过，发现这一结果却完全是另一回事，从欧拉首次研究这一问题开始到他发现下列恒等式为止，当中一共经过了十三年时间，就可说明这一点(几乎所有的恒等式一经有人写出就都显而易见)：

$$\begin{aligned}(a^2+b^2+c^2+d^2)(r^2+s^2+t^2+u^2)\\=(ar+bs+ct+du)^2+(as-br+cu-dt)^2\\+(at-bu-cr+ds)^2+(au+bt-cs-dr)^2,\end{aligned}$$

乘出来即可验证此式. (注意，右端乘出后的各项 a^2r^2, a^2s^2, …, d^2u^2, 也出现在左端乘出后的结果中，而且，凭观察也不难看出，所有的交叉乘积项均会消失.)

由引理 1 可知，要证明每个正整数都是四平方数之和，我们只需表明每个素数都是四平方数之和就行了. 例如，由

$$37=6^2+1^2+0^2+0^2,\qquad 57=7^2+2^2+2^2+0^2,$$

我们可得

$$\begin{aligned}2109=57\cdot37=(6\cdot7+1\cdot2+0\cdot2+0\cdot0)^2\\+(6\cdot2-1\cdot7+0\cdot0-0\cdot2)^2+(6\cdot2\\-1\cdot0-0\cdot7+0\cdot2)^2+(6\cdot0+1\cdot2-0\cdot2-0\cdot7)^2\\=44^2+5^2+12^2+2^2.\end{aligned}$$

与此相似，我们可将任一整数分解为一些素数的乘积，而且要是我们知道了每一素数的四平方之和的表示式，我们就可求得这个整数的四平方之和的表示式.

引理 2 若 p 是一个奇素数，则

$$1+x^2+y^2\equiv0(\bmod p)$$

必有一组解，它们满足 $0\leqslant x<p/2$ 和 $0\leqslant y<p/2$.

证明 下列集合中各数互不相同$(\bmod p)$：

$$S_1=\left\{0^2,\ 1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2\right\}.$$

(这是因为，由 $x^2\equiv y^2 \pmod p$ 可得 $x\equiv\pm y \pmod p$.）因而，下列集合中各数也互不相同 $(\bmod\ p)$:

$$S_2=\left\{-1-0^2,\ -1-1^2,\ -1-2^2,\ \cdots,\ -1-\left(\frac{p-1}{2}\right)^2\right\}.$$

S_1 和 S_2 合在一起共有 $(p-1)/2+1+(p-1)/2+1=p+1$ 个数. 由于只有 p 个最小剩余 $(\bmod p)$, 故 S_1 中必有一数与 S_2 中一数同余，即对某 x 和 y, 有

$$x^2\equiv -1-y^2 \pmod p,$$

其中，$0\leqslant x\leqslant (p-1)/2$, $0\leqslant y\leqslant (p-1)/2$.

欲证每一正整数是四平方数之和，我们即将采用的证明方法与证明整数表为两平方数之和的有关定理所用的方法相同，即先将 p 的某个倍数表为四平方数之和，然后作出 p 的一个更小的倍数，它也为四平方数之和，多次重复这一步骤，直到将 p 表为四平方数之和为止，而这就是我们需要证明的一点. 由于 $2=1^2+1^2+0^2+0^2$, 故 $p=2$ 的情况已经解决，因而我们可以假定 p 为奇素数.

引理 3 对每个奇素数 p, 必存在一个奇数 m, $m<p$, 使下列方程有解:

$$mp=x^2+y^2+z^2+w^2.$$

证明 由引理 2 我们知，对某一 k, 存在 x 和 y, 使

$$kp=x^2+y^2+1^2+0^2.$$

由于 $0\leqslant x<p/2$, $0\leqslant y<p/2$, 我们有

$$kp=x^2+y^2+1<p^2/4+p^2/4+1<p^2,$$

故 $k<p$. 剩下来只需证明，k 可假定为奇数. 设

$$kp=x^2+y^2+z^2+w^2,$$

且 k 为偶数，则 x, y, z, w 或全为奇数，或全为偶数，或二个为奇数、二个为偶数. 无论出现哪种情况，我们总可调整各项，使

$$x \equiv y \pmod 2, \quad z \equiv w \pmod 2.$$

因此，

$$\frac{kp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2.$$

若 $k/2$ 为偶数，我们重复上述步骤可将 $(k/4)p$ 表为四平方数之和. 由于 $k \neq 0$, 最后必得一数，它是 p 的奇数倍，且已表为四平方数之和.

【练习 1】 由

$$12 \cdot 17 = 204 = 14^2 + 2^2 + 2^2 + 0^2,$$
$$12 \cdot 17 = 204 = 13^2 + 5^2 + 3^2 + 1^2,$$

求 $3 \cdot 17$ 的四平方数之和的表示式.

引理 4 若 m 和 p 为奇数，$1 < m < p$, 且

$$mp = x^2 + y^2 + z^2 + w^2,$$

则存在正整数 m_1, $m_1 < m$, 使

$$m_1 p = x_1^2 + y_1^2 + z_1^2 + w_1^2,$$

其中 x_1, y_1, z_1, w_1 均为整数.

证明 象在"二平方和"定理中所作的那样，我们着手从 x, y, z, w 构造出 x_1, y_1, z_1, w_1. 选取 A, B, C, D, 使

$$A \equiv x, \quad B \equiv y, \quad C \equiv z, \quad D \equiv w \pmod m,$$

且每一数都严格地介于 $-m/2$ 与 $m/2$ 之间，也即 A, B, C, D 在数值上都是 x 的最小剩余$\pmod m$. 因而，

$$A^2 + B^2 + C^2 + D^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod m.$$

所以，对某 k 有

$$A^2 + B^2 + C^2 + D^2 = km.$$

由于

$$A^2 + B^2 + C^2 + D^2 < m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2,$$

我们得 $0<k<m$. （若 $k=0$, 则 m 整除 x, y, z, w 中的每一个，故 $m^2|mp$, 这是不可能的，因为 $1<m<p$.）于是，

$$\begin{aligned} m^2kp &= (mp)(km) \\ &= (x^2+y^2+z^2+w^2)(A^2+B^2+C^2+D^2). \end{aligned}$$

而由引理 1, 我们得

$$\begin{aligned} m^2kp = &(xA+yB+zC+wD)^2+(xB-yA+zD-wC)^2 \\ &+(xC-yD-zA+wD)^2+(xD+yC-zB-wA)^2. \end{aligned}$$

这些括号内的数均可被 m 整除：

$$\begin{aligned} &xA+yB+zC+wD \equiv x^2+y^2+z^2+w^2 \equiv 0 \pmod m, \\ &xB-yA+zD-wC \equiv xy-yx+zw-wz \equiv 0 \pmod m, \\ &xC-yD-zA+wB \equiv xz-yw-zx+wy \equiv 0 \pmod m, \\ &xD+yC-zB-wA \equiv xw+yz-zy-wx \equiv 0 \pmod m. \end{aligned}$$

这样，若我们记

$$\begin{aligned} x_1 &= (xA+yB+zC+wD)/m, \\ y_1 &= (xB-yA+zD-wC)/m, \\ z_1 &= (xC-yD-zA+wB)/m, \\ w_1 &= (xD-yC-zB-wA)/m, \end{aligned}$$

我们就有 $\qquad x_1^2+y_1^2+z_1^2+w_1^2=(m^2kp)/m^2=kp.$

因 $k<m$, 引理得证.

定理 1 每个正整数均可写为四个整数的平方和.

证明 假定 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. 从引理 3 出发，反复应用引理 4, 对每一 i 可得 $p_i=x^2+y^2+z^2+w^2$ 的解. 由引理 1, 对每一 i, $p_i^{e_i}$ 都可写成四平方数之和. 再用引理 1(k 次), 我们即能求得 $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ 表为四平方数之和的表示式.

习 题

1. 将小于或等于 23 的各个素数表为四平方数之和.

2. 将下列各数分别表为四平方数之和：(a) 121；(b) 391；(c) 47321.

3. 将 5,724,631 表为四平方数之和.

4. 根据 $53=7^2+2^2+0^2+0^2$ 和欧拉公式（引理1），求 $18179=7^3\cdot 53$ 写为四平方数之和的一个表示式.

5. 若 $8|(x^2+y^2+z^2+w^2)$，证明 x, y, z, w 均为偶数.

6. 若 $n=x^2+y^2+z^2+w^2$，证明：重排次序并适当选取符号后，总可使 $x+y+z$ 成为 3 的倍数.

7. 在 10, 11, 12, …, 20 这些整数中，哪些数能唯一地表为四平方数之和（相加的各个平方数的次序可以不同）？

8. 若 $n=x^2+y^2+z^2+w^2$，x, y, z, w 均为非负数，证明 $\min(x, y, z, w) \leqslant n^{1/2}/2 \leqslant \max(x, y, z, w) \leqslant n^{1/2}$.

9. 由 $2\cdot 17\cdot 1973=67082=238^2+102^2+5^2+3^2$，将 $17\cdot 1973$ 表示为四平方数之和.

10. 下面是欧拉原来对引理2的证明，补上没有详细写出的地方：假定 $(-1/p)=1$，则存在一个整数 x，使 $1+x^2\equiv 0 \pmod p$. 假定 $(-1/p)=-1$，且引理不真，那么，$1+1-2=0$ 表明 $(-2/p)=-1$，因而 $(2/p)=1$. 而 $1+2-3=0$ 表明，$(-3/p)=-1$，即 $(3/p)=1$. 于是，1, 2, …, $p-1$ 全为二次剩余 $(\bmod p)$.

11. 若 $n>0$，$8|n$，证明 n 不可能是八个以下的奇数的平方和.

12. 若 t 为偶数，x, y, z 无大于 1 的公因子，证明不可能成立

$$t^2=x^2+y^2+z^2.$$

§ 20 $x^2-Ny^2=1$

丢番图方程的理论尚不完备，我们还没有多少定理可以用之于一类非常广泛的方程．通常，特殊的方程要用特殊的方法来研究，求解一个方程的方法用于求解另一方程，可能会毫无价值．另一方面，一种方法有时也可能对两个方程都适用．一个完好的定理，如果用于考察任一丢番图方程，应使我们能够判定方程是否有解；如果这个定理还能精确地告诉我们方程共有多少解，那就更好；要是它还能告诉我们这些解是什么，那就更为理想了．看来，这一理想也许永远不能实现[注]．这里介绍目前已经清楚的一个相当一般的定理．

定理 设

$$F(x,\ y)=a_nx^n+a_{n-1}x^{n-1}y+a_{n-2}x^{n-2}y^2+\cdots+a_0y^n,$$

且 $F(x,\ 1)=0$ 没有重根，则当 $n\geqslant 3$ 时，方程

$$F(x,\ y)=C\quad（其中 C 是一个整数）$$

只有有限多组解．

特殊地，这一定理表明，当 $n\geqslant 3$ 时，$ax^n+by^n=c$ 一般只能有有限多组解．那么，要是 $n<3$ 呢？我们在线性不定方程一节中已经透彻地分析了 $n=1$ 时的情况．对于 $n=2$，我们在毕达哥拉斯三角形一节里考虑了一种特殊的情况，而 $n=2$ 时

［注］ 在希尔伯特 (Hilbert)23 个著名的数学问题中，第十个问题就是：有没有一个算法可以用来判定任一丢番图方程是否有解？ 1970 年，这个问题已获得解决，答案是否定的．这也是数理逻辑研究中的一个重大成果．——译校者注

的一般情况就太复杂了，难以在此讨论．本节中，我们要研究另一种特殊的情况：

$$x^2-Ny^2=1.$$

我们将要证明，若能找到此方程使$x>1$的一组解，就能求出它的无限多组解．事实上，若能求出最小的一组解(即满足 $x>1$ 的尽可能小的一组解)，那么我们就能求得此方程的所有解．

方程 $x^2-Ny^2=1$ 通常称为佩尔(Pell)方程，这是由欧拉的误会引起的．由于欧拉是这样称呼的，而欧拉太有名了，从此大家就这样叫了．但是，佩尔从未解过这一方程，甚至他能否解出这个方程也值得怀疑．因此，我们要一反通常的叫法，而把 $x^2-Ny^2=1$ 称为费马方程．

无论 N 取什么值，$x=\pm1$ 和 $y=0$ 总满足此方程，我们把 x 和 y 中有一为零的解称为平凡解．

【练习 1】 用尝试法分别求出 $x^2-2y^2=1$ 和 $x^2-3y^2=1$ 的一组非平凡解．

用尝试法求 $x^2-Ny^2=1$ 的一组非平凡解，一种有效的方法是，对 $y=1, 2, \cdots$ 造出 $1+Ny^2$ 的一张表，然后找出平方数来．此时，表 B 可能会有些帮助．

求解 $x^2-Ny^2=1$ 时，N 取负值的情况可不用考虑．当 $N\leqslant-2$ 时，此方程显然只有使 $y=0$ 的平凡解，因为左端两项均为非负．对于 $N=-1$，还有解：$x=0$，$y=\pm1$，它们也是平凡解．除了假设 N 为正数外，我们还可假定 N 不是平方数．如果它是平方数，则对某个 m，有 $N=m^2$．我们有

$$1=x^2-m^2y^2=(x-my)(x+my).$$

两个整数之积要为 1，只有两数均为 1 或均为 -1 才行，因此要迅速求出所有解，只需解两组线性方程即可．

【练习 2】(选做) 证明 $x^2-m^2y^2=1$ 的解只能是$x=\pm1$，

$y=0$.

下面我们就假定 $N>0$ 且 N 不是平方数. 有了这一假定，总可证明，$x^2-Ny^2=1$ 必有不同于 $x=\pm1$, $y=0$ 的解. 我们不作证明而承认这一点. 非平凡解的存在性证明有两种方法: 一种方法要用到连分数的许多性质; 另一种方法较长，由狄利克雷(Dirichlet)在1842年首次提出，他改进了拉格朗日在1766年给出的一个证明.

由于 $x^2-Ny^2=(x+y\sqrt{N})(x-y\sqrt{N})$，所以形为 $x+y\sqrt{N}$ 的无理数与费马方程的解有着密切的联系，它们有好几条重要的性质，我们在下面各引理中将予以介绍. 当且仅当 r 和 s 均为整数且 $r^2-Ns^2=1$ 时，我们称 $\alpha=r+s\sqrt{N}$ 给出了 $x^2-Ny^2=1$ 的解. 例如，$3+2\sqrt{2}$ 给出了 $x^2-2y^2=1$ 的一组解，$8+3\sqrt{7}$ 给出了 $x^2-7y^2=1$ 的一组解.

引理 1 若 $N>0$ 不是平方数，则

$$x+y\sqrt{N}=r+s\sqrt{N}$$

的充要条件为 $x=r$ 和 $y=s$.

证明 若 $x=r$, $y=s$, 显然有 $x+y\sqrt{N}=r+s\sqrt{N}$. 因此，重要的是其逆. 为了证明其逆，假定 $x+y\sqrt{N}=r+s\sqrt{N}$，但 $y\neq s$. 则

$$\sqrt{N}=\frac{x-r}{s-y}$$

是一个有理数. 但因 N 不是平方数，故 $\sqrt{N}$ 是无理数，便得矛盾. 因此，$y=s$, 从而 $x=r$.

引理 2 对任意整数 a, b, c, d, N, 有

$(a^2-Nb^2)(c^2-Nd^2)=(ac+Nbd)^2-N(ad+bc)^2$.

证明 乘出即知.

【练习 3】 已知: $2^2-3\cdot1^2=1$, $7^2-3\cdot4^2=1$, 用引理 2

求 $x^2-3y^2=1$ 的另一组解.

引理 3 若 α 给出 $x^2-Ny^2=1$ 的一组解，则 $1/\alpha$ 给出它的另一组解.

证明 设 $\alpha=r+s\sqrt{N}$，则我们知 $r^2-Ns^2=1$，故有

$$\frac{1}{\alpha}=\frac{1}{r+s\sqrt{N}}\cdot\frac{r-s\sqrt{N}}{r-s\sqrt{N}}=\frac{r-s\sqrt{N}}{r^2-Ns^2}=r-s\sqrt{N},$$

因 $r^2-N(-s)^2=1$，故引理得证.

引理 4 若 α 和 β 给出 $x^2-Ny^2=1$ 的解，则 $\alpha\beta$ 也给出它的解.

证明 设 $\alpha=a+b\sqrt{N}$，　$\beta=c+d\sqrt{N}$，则

$$\begin{aligned}\alpha\beta&=(a+b\sqrt{N})(c+d\sqrt{N})\\&=(ac+Nbd)+(ad+bc)\sqrt{N}.\end{aligned}$$

而由引理 2，我们得

$$\begin{aligned}&(ac+Nbd)^2-N(ad+bc)^2\\&\quad=(a^2-Nb^2)(c^2-Nd^2)=1,\end{aligned}$$

这就说明，$\alpha\beta$ 给出了方程的解.

引理 5 若 α 给出 $x^2-Ny^2=1$ 的一组解，则无论 k 是正数、负数还是零，α^k 也给出方程的解.

【练习 4】 证明引理 5.（首先用引理 4 和归纳法证明引理 5 对所有 $k\geqslant1$ 成立，然后用引理 3 证明它对 $k\leqslant-1$ 亦成立，最后考虑 $k=0$ 的情况.）

引理 5 表明，若我们知道了一个数 α，$\alpha>1$，它给出 $x^2-Ny^2=1$ 的一组解，则我们就能找到无限多组解，它们都可由 α^k 给出，$k=2, 3, \cdots$. 而且，这些解互不相同，因为对所有 k，$\alpha^{k+1}>\alpha^k$. 例如，$3+\sqrt{2}$ 给出了 $x^2-2y^2=1$ 的一组解，则

$$(3+2\sqrt{2})^2=17+12\sqrt{2},$$

$$(3+2\sqrt{2})^3=(17+12\sqrt{2})(3+2\sqrt{2})=99+70\sqrt{2},$$

和 $3+2\sqrt{2}$ 的更高次乘幂都给出此方程的解.

【练习 5】 验证 $(3+2\sqrt{2})^2$ 和 $(3+2\sqrt{2})^3$ 给出了 $x^2-2y^2=1$ 的解.

【练习 6】 $\alpha=2+\sqrt{3}$ 给出了 $x^2-3y^2=1$ 的一组解，求出另外两组非平凡解来.

引理 6 假定 a, b, c, d 均为非负数，$\alpha=a+b\sqrt{N}$ 和 $\beta=c+d\sqrt{N}$ 分别给出 $x^2-Ny^2=1$ 的解，则当且仅当 $a<c$ 时，有 $\alpha<\beta$.

证明 假定 $a<c$，则 $a^2<c^2$. 又因 $a^2=1+Nb^2$, $c^2=1+Nd^2$，故有 $Nb^2<Nd^2$. 因为 b, d, N 均不为负数，可得 $b<d$. 与 $a<c$ 一起，便得 $\alpha<\beta$. 又假定 $\alpha<\beta$. 若有 $a\geqslant c$，则 $a^2\geqslant c^2$. 由此可得 $b^2\geqslant d^2$，这就说明 $\alpha\geqslant\beta$，这是不可能的. 故必有 $a<c$.

现在我们就可以讨论 $x^2-Ny^2=1$ 的所有解了. 考虑所有能够给出 $x^2-Ny^2=1$ 的解的实数集合. 设 θ 是此集合中大于 1 的最小数. 应注意到，引理 6 保证了这样一个最小元是存在的，因为此集合中的一些数 $r+s\sqrt{N}$ 可以根据 r 的大小排列起来，而 r 为整数，且任何正整数的非空集合必有最小元. 我们将 θ 称作 $x^2-Ny^2=1$ 的生成元，并来证明

定理 1 若 θ 是 $x^2-Ny^2=1$ 的生成元，则 $\theta^k(k=1,2,\cdots)$ 给出了此方程使 x 和 y 取正值的所有非平凡解.

注意，将 x 和 y 限制取正值并不会使我们失去任何重要的东西，因为非平凡解总是四对为一批地出现的:

$$\{(x, y), (x, -y), (-x, y), (-x, -y)\},$$

其中恰有一组解具有两个正数. 还应注意，我们没有提及生成元的存在性，事实上，正如我们刚才说过的，这样一个数总是可以找到的. 根据 $\sqrt{N}$ 的连分数展开式用一种方法可容易

地算出 θ 来. 说"容易"是指计算机可以毫不费事地进行这一计算. 事实上, 对某些 N 的值, 这种计算是非常枯燥乏味的. 当然, 一个生成元也可用尝试法求出, 而且在很长一段时间内这曾是唯一可用的方法. 在十七世纪, 曾有一位印度数学家说过, 要是有人能在一年的时间内解出 $x^2-92y^2=1$, 他就可算得上是一名真正的数学家. 算不算真正的数学家尚可商榷, 但这样一个人至少称得上是一位真正的算术家, 因为此方程的生成元是 $1151+120\sqrt{92}$. 即使对 $x^2-29y^2=1$ 这样一个看起来是如此简单的方程, 要是用尝试法来求解的话, 任务也会非常艰巨, 它的最小非平凡正数解为 $x=9801$, $y=1820$. 对于 $x^2-61y^2=1$ 这一方程, 我们要一直取到 $x=1766319049$ 和 $y=226153980$ 时, 才会得到非平凡解. 如果你有兴趣的话, 你可以用乘法来验证这是一组解.

定理 1 的证明 设 $x=r$, $y=s$ 是 $x^2-Ny^2=1$ 的任意一组非平凡解, 其中 $r>0$, $s>0$. 令 $\alpha=r+s\sqrt{N}$. 我们要证明, 存在某 k, 使 $\alpha=\theta^k$. 由生成元的定义可知, $\alpha\geqslant\theta$, 故有整数 k, 使

$$\theta^k\leqslant\alpha<\theta^{k+1}.$$

于是, $1\leqslant\theta^{-k}\alpha<\theta$. 由引理 4 和引理 5, 我们知 $\theta^{-k}\alpha$ 给出 $x^2-Ny^2=1$ 的一组解. 我们已把 θ 定义为给出非平凡解且大于 1 的最小数. 但 $\theta^{-k}\alpha$ 比 θ 要小, 却给出了方程的解, 因而 $\theta^{-k}\alpha$ 给出的一定是平凡解, 故 $\theta^{-k}\alpha=1$, 即 $\alpha=\theta^k$. 这就是我们欲证之结论.

习　题

1. 当 N 为下列各数时, 求 $x^2-Ny^2=1$ 的生成元: (a) 6; (b) 7; (c) 8; (d) 10; (e) 11; (f) 12.

孙

2. 当 N 为下列各数时，分别求出 $x^2-Ny^2=1$ 的两组正的非平凡解:
(a) 6; (b) 8; (c) 12; (d) 14; (e) 63; (f) 99.

3. 求出 $x^2+2xy-2y^2=1$ 的三组非平凡解.

4. 求出题 3 中的方程的无限多组解.

5. (a) 证明: 若 $a^2>b$, 且 a^2-b 不是平方数, 则 $x^2+2axy+by^2=1$ 有无限多组解;
(b) 若 $a^2<b$,证明在(a)中的方程的所有解中,都有 $y=0,1$, 或 -1;
(c) 若 $a^2=b$,会发生什么情况呢?

6. (a) 设 $a=2mn$, $b=m^2-n^2$, $c=m^2+n^2$ 是一个毕达哥拉斯三角形的三条边,假定 $b=a+1$. 证明 $(m-n)^2-2n^2=1$, 并求出所有这样的三角形;
(b) 求出这种三角形中的最小的两个.

7. (a) 证明: 当且仅当 $3(a^2-1)$ 是平方数时, 以 $2a-1$, $2a$, $2a+1$ 为三边的三角形的面积是整数;
(b) 找出三个这样的三角形;
(c) 当且仅当 $3((2a+1)^2-4)$ 为平方数时, 以 $2a$, $2a+1$, $2a+2$ 为三边的三角形的面积是有理数;
(d) 证明上述情况是不可能存在的.

8. 证明: 若 $x_1+y_1\sqrt{N}$ 是 $x^2-Ny^2=1$ 的生成元, 则所有解 x_k, y_k 的形式可写为
$$2x_k=(x_1+y_1\sqrt{N})^k+(x_1-y_1\sqrt{N})^k,$$
$$2\sqrt{N}y_k=(x_1+y_1\sqrt{N})^k-(x_1-y_1\sqrt{N})^k.$$

9. 证明: 若 $x_1+y_1\sqrt{N}$ 是 $x^2-Ny^2=1$ 的生成元, 则
$$0<x_1-y_1\sqrt{N}<1.$$

10. 参照题 8 和题 9 所用的记号, 当 k 愈来愈大时, x_k/y_k 将怎样变化?

11. 若 $x_k+y_k\sqrt{2}=(3+2\sqrt{2})^k$, 对 $k=1, 2, 3, 4$, 分别计算 $(x_k/y_k)-\sqrt{2}$. ($\sqrt{2}=1.414213562\cdots$.)

12. (a) 证明: 当 $N\equiv 3 \pmod 4$ 时, $x^2-Ny^2=-1$ 无解;
(b) 证明: 若 x_1, y_1 为 $x^2-Ny^2=-1$ 的一组解, 且 $x_1>1$, 则 u_k, v_k $(k=1, 2, \cdots)$ 是 $x^2-Ny^2=1$ 的解, 其中
$$u_k+v_k\sqrt{N}=(x_1+y_1\sqrt{N})^{2k}.$$

13. 证明：若 $x^2-Ny^2=k$ 有一组解，它就有无限多组解.

14. $10^2+11^2+12^2=13^2+14^2$. 找出另一个例子，使三个相继整数的平方和等于另外两个相继整数的平方和.

15. 证明：当 $n>0$ 时，$1+n+n^2$ 决不会是平方数.

16. 若 $x_1+y_1\sqrt{N}$ 是 $x^2-Ny^2=1$ 的生成元，且对 $k=1, 2, \cdots$，有 $x_k+y_k\sqrt{N}=(x_1+y_1\sqrt{N})^k$，证明

$$x_{k+1}=2x_1x_k-x_{k-1},$$
$$y_{k+1}=2x_1y_k-y_{k-1}.$$

17. 用题 16 的方法为题 11 中求得的逼近 $\sqrt{2}$ 的有理数序列再增添一项.

§ 21　关于素数的公式

在数学发展的先前一个时期中，人们曾以为“函数”和“公式”两词的含义多少有点相同．今天，函数的概念则更为一般，但若一个函数有一个明显的公式可供查看，我们中仍有许多人会感到舒服一点．下面两种说法实际上并无区别：

“$f(n)$表示n的最大素因子”；

$$“f(n)=\lim_{r\to\infty}\lim_{s\to\infty}\lim_{t\to 0}\sum_{u=0}^{s}(1-\cos^2(u!)^r\pi/n)^{2t}”.$$

第一种说法更为简单，但第二种说法或许会使我们感到这个f更易于掌握一些．

公式之所以重要，当然并非出于人们心理上的需要，而是因为它在实际中有用．一般说来，一个公式应使我们能够算出我们关心的事．因此，上面那个公式就没有用文字叙述出来的那句话来得有用，因为它不但无助于计算，而且反而使f更为含糊．不过，要是我们认为公式在一般情况下是件好事并觉得最好有个公式的话，那么花点力气去找一找还是无可非议的．我们或许想找一找第n个素数p_n的公式，但素数却如此杂乱无章地散布在整数中，甚至原因也可能说不清楚．这件事既然办不到，那么最好能够找到一个公式，由它得出的数都是素数．本节的目的就在于首先证明，不存在一个非常简单的公式，特别是不存在一个用多项式表示的公式，可以做到这一点；其次还要提出一个公式，即$f(n)=[\theta^{3^n}]$，它对所有$n(n=1, 2, 3, \cdots)$都能得出素数，但是，遗憾得很，它却无

法用于计算.

考虑起来最简单的一种公式是

$$f(n)=an+b.$$

如若我们找到了这样一个函数,它给出的数全为素数,那么我们就会得到一个算术级数,各项全为素数,公差为a. 查一查整个素数表,我们可以发现许多由素数构成的算术级数,但其中没有一个是无限的,例如:

3, 5, 7;

7, 37, 67, 97, 127, 157;

199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089.

【练习 1】 若$an+b$对两个不同的n值均为素数,证明a与b互素.

【练习 2】(选做) 若$2\nmid a$,证明:对两个以上相继的n值,$an+b$不可能都为素数.

尽管有上述一些局部性结果,我们现在却要证明,任何算术级数都不会只产生素数.假定$an+b=p$,p是一个素数.令$n_k=n+kp$,$k=0, 1, \cdots$ 则级数的第n_k项为

$$an_k+b=a(n+kp)+b=(an+b)+akp=p+akp,$$

对任何k它都能被p整除.于是级数各段的第p项均被p整除(因为这些n_k每隔p个数出现一次),因而此级数包含了无限多个合数.

数列$\{an+b\}$中不可能全为素数,但很自然地要问:它是否包含了无限多个素数呢?狄利克雷定理给出了答案:若$(a, b)=1$,则$\{an+b\}$包含有无限多个素数.例如,数列$\{4n+1\}$中,就有素数5, 13, 17, 29, 37, 41, …;数列$\{12n+7\}$中,有7, 19, 31, 43, 67, ….狄利克雷定理说明,在这

两个数列中，我们永远找不到最后的素数．$(a, b)=1$ 这个条件显然是必要的：$\{6n+3\}$ 只含有一个素数，$\{6n+4\}$ 中一个素数也没有．狄利克雷的重大成果就在于证明，这个条件也是充分的．这一定理的证明绝非易事，我们就不想证了．进一步说，我们不仅可证数列 $\{an+b\}$（其中 $(a, b)=1$）中存在无限多个素数，而且还能估计出这些素数的分布情况，在这个数列中，小于 N 的素数个数大致上等于 $N/\phi(a)\log N$，其中 ϕ 表示欧拉函数．

现在我们来证一个定理，它说明了算术级数的特性有点象整数序列，而且还能使我们看出一个级数可以包含着多少个全为素数的相继的项．

定理 1 若 $p\nmid a$，则序列 $\{an+b\}$ 经过分段，可使各段的第 p 项都能被 p 整除．

证明 因 $p\nmid a$，故 p 与 a 互素，即有整数 r 和 s 使 $pr+as=1$．令

$$n_k=kp-bs, \quad k=1, 2, \cdots,$$

则

$$\begin{aligned}an_k+b&=a(kp-bs)+b=akp-bas+b\\&=akp-b(1-pr)+b=akp-b+bpr+b\\&=p(ak+br).\end{aligned}$$

因此，对每一 k，$k=1, 2, \cdots$，有 $p\mid(an_k+b)$．因 $n_{k+1}-n_k=p$，故 an_k+b 每隔 $p-1$ 项出现一次．

由定理 1 可得，若 $2\nmid a$，则序列 $\{an+b\}$ 中每隔一项就有一数被 2 整除．因而该序列不可能相继地有四项或更多的项都不是合数，而且若有相继的三项都不是合数，则其第二项必定是 2．一般地，若 $p\nmid a$，则 $\{an+b\}$ 中不可能相继地出现 $2p-1$ 个以上的项都不是合数，而且要是相继地出现 $2p-1$ 项都不是合数，则位于其中间的那个数必为 p；而在其它情况

下，至多只能有 $p-1$ 个相继的项均非合数．于是，若我们要找一个算术级数，使它包含12个相继出现的素数，公差 a 就不能随便选取．要是2，3，5，7，11在级数中不出现，公差就应被 $2\cdot3\cdot5\cdot7\cdot11=2310$ 整除．至今所知，最长的全为素数的算术级数一共有16项：

$$223092870n+2236133941 \quad (n=0,\ 1,\ \cdots,\ 15).$$

既然线性公式不能当作只生成素数的函数，下一次要试的就是二次函数：an^2+bn+c 能对所有整数 n 都是素数吗？我们同样能够获得某些结果．例如，若 $f(n)=n^2+21n+1$，则当 $n=-38,\ -37,\ \cdots,\ 17$（这串数一共由56个相继的整数所组成）时，$f(n)$ 都不是合数．但 $f(18)=703=37\cdot19$．（注意："不是合数"并非"素数"的同义词，如1既不是合数也不是素数．因 $f(0)=1$，故我们不能说 $f(n)$ 对这56个相继的整数都是素数．）

【练习3】 利用同余式证明：上述 $f(n)$ 对任何 n 均有，$2\nmid f(n)$，$3\nmid f(n)$，$7\nmid f(n)$．

【练习4】 证明：若 $n\equiv-1 \pmod{19}$，则 $19\mid f(n)$．

【练习5】（选做） 证明：仅当 $n\equiv-1 \pmod{19}$ 时，$19\mid f(n)$．

含有很多素数的二次函数的另一个著名例子为 n^2+n+41，它对于80个相继整数：$n=-40,\ -39,\ \cdots,\ 39$，不仅都不是合数，而且都是素数．目前，它还是冠军：还不知有哪个二次函数能一连串地产生80个以上的数都不是合数．鉴于素数随着整数的增大而渐趋稀疏，因此也不是没有理由猜想，再也不会有别的二次函数能够相继地产生80个以上的数都不是合数了．要在近期内解决这一猜想，希望是渺茫的．目前已经知道的是，形为 $n^2+n+A\,(A>41)$ 的二次函数中，没有

哪一个能对 $n=0, 1, \cdots, A-2$ 全都给出素数，这是从1967年才得到证明的一个很难的结果中推知的.

任何二次函数都不可能只给出素数. 设

$$f(n)=an^2+bn+c=p$$

对某 n 是素数，也即 $an^2+bn+c\equiv 0 \pmod p$. 令 $n_k=n+kp$, $k=0, 1, \cdots$, 则

$$f(n_k)=a(n+kp)^2+b(n+kp)+c$$
$$=an^2+2ankp+ak^2p^2+bn+bkp+c,$$

即 $$f(n_k)\equiv an^2+bn+c\equiv 0 \pmod p).$$

故对任一 k, $f(n_k)$ 都能被 p 整除. 因此,序列 $\{an^2+bn+c\}$ 分段后,每段的第 p 项就都能被 p 整除,故此序列包含了无限多个合数.

我们已经知道了狄利克雷定理，也许就想问一问：要是 a, b, c 无大于1的公因子，$\{an^2+bn+c\}$ 是否包含有无限多个素数呢？对于二次函数，还没有与狄利克雷定理相应的定理. 事实上，至今尚未证明，n^2+1 能无限次地成为素数，虽然看起来不大可能会不是如此.

我们也许已经发觉,用三次多项式来代表素数,并不会比二次多项式要好. 这是正确的. 若 f 是一个任意次多项式,若对某一 n, $f(n)=p$ 是素数,则可以证明,对所有 k, $k=0, 1, \cdots$，必有 $p|f(n+kp)$. 其证明与一次多项式和二次多项式的情况完全相同. 此外,还已经知道，若 f 和 g 均为多项式，那么，除非当 n 充分大时 $[f(n)/g(n)]$ 变成了常数，否则 $[f(n)/g(n)]$ 也不可能对所有 n 都给出素数.

另一方面,我们可以造出一个多项式,它能相继地给出我们所需数量的素数值，因为我们可证，根据 $d+1$ 个任意给定的值,总可以造出一个 d 次多项式. 例如,若

$$60f(x)=7x^5-85x^4+355x^3-575x^2+418x+180,$$

则我们有

n	0	1	2	3	4	5
$f(n)$	3	5	7	11	13	17.

可造出一个类似的多项式取 81 个相继素数的值，但其次数将是 80.

我们放弃了多项式，很自然地会想用指数函数来试一试. 例如，若

$$f(n)=[(3/2)^n],$$

则对 $n=2, 3, 4, 5, 6, 7$, $f(n)$ 全为素数（其函数值分别为 2, 3, 5, 7, 11, 17），但 $f(8)=25$, 而且这一串数中下一个素数将是 $f(21)=4987$. 谁也没有证明过，象 $f(n)=[\theta^n]$ 这样一个公式不能总给出素数，我们也不知道 $[\theta^n]$ 是否会无限次地给出素数. 这样一些问题看来是极为困难的.

不过，也的确存在一些可用简单公式表出的函数，它们总代表素数. 我们将介绍穆尔士 (Mills) 的一个引人注目的结果，并且部分地给出证明.

定理 2 存在一个实数 θ, 使 $[\theta^{3^n}]$ 对所有 $n(n=1, 2, \cdots)$ 都为素数.

我们将看到，这一定理所包含的内容并不如它的外表那样瞩目. 在我们将它的证明完成后，就更会感到它并不那么值得令人注目了. 证明中给出了 θ 的构造方法，但这一方法却依赖于能否识别出任意大的素数；但要是我们已能识别出任意大的素数，也就没有必要找出一个公式了.

证明中，我们要用到数学分析中的两个定理.

定理 若序列 $u_1, u_2, u_3, \cdots, u_n, \cdots$ 上有界且非下降，则当 n 无限增大时，此序列必有一个极限 θ.

换句话说，若有一数 M 使对所有的 n 有 $u_n<M$, 且对所

有 $n(n=1, 2, \cdots)$ 有 $u_n \leqslant u_{n+1}$，则存在一数 θ，当 n 无限增大时，θ 与 u_n 之差变得任意地小．这个定理和下面的定理我们都不证了．

定理 若序列 $v_1, v_2, v_3, \cdots, v_n, \cdots$ 下有界且非上升，则当 n 无限增大时，此序列必有一个极限 ϕ．

我们将记

$$\lim_{n\to\infty} u_n = \theta, \quad \lim_{n\to\infty} v_n = \phi,$$

前面一式读为"当 n 趋向于无穷大时 u_n 的极限为 θ"，对后一式也有相应的读法．

定理 2 的证明 此证明还依赖于下列定理：存在一个整数 A，当 $n>A$ 时，就有一个素数 p 满足

$$(1) \qquad n^3 < p < (n+1)^3 - 1.$$

这个定理我们将不予证明，它的证明依赖于黎曼(Riemann)ζ 函数的深刻性质．我们将用 (1) 来求出素数的一个序列，并进而求出 θ．设 p_1 是大于 A 的任一素数，而对 $n=1, 2, \cdots$，令 p_{n+1} 为满足下式的素数：

$$(2) \qquad p_n^3 < p_{n+1} < (p_n+1)^3 - 1.$$

鉴于(1)，对每个 n，这样的素数都存在．设

$$(3) \qquad u_n = p_n^{3^{-n}}, \quad v_n = (p_n+1)^{3^{-n}},$$

$n=1, 2, \cdots$．我们看到，当 n 增加时，u_n 也增加，这是因为，由(2)，

$$(4) \qquad u_{n+1} = p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}} = p_n^{3^{-n}} = u_n.$$

又，$\{v_n\}$ 是下降序列，因为由(2)，

$$(5) \qquad v_{n+1} = (p_{n+1}+1)^{3^{-n-1}} < ((p_n+1)^3 - 1 + 1)^{3^{-n-1}} = (p_n+1)^{3^{-n}} = v_n.$$

由(3)显然知，$u_n < v_n$．因此，由于(5)，得

$$u_n < v_n < v_{n-1} < \cdots < v_1,$$

故对所有 n, $u_n<v_1$. 同样, 由(4)我们有

$$v_n>u_n>u_{n-1}>\cdots>u_1,$$

故对所有 n, $v_n>u_1$. 这样, $\{u_n\}$ 就是以 v_1 为上界的上升序列, 因而 $\{u_n\}$ 有一极限, 把它叫做 θ. 同时, $\{v_n\}$ 是以 u_1 为下界的下降序列, $\{v_n\}$ 也有一个极限, 把它叫做 ϕ. 由于对所有 n, 有 $u_n<v_n$, 因此 $\theta\leqslant\phi$. 事实上, 由于 $\{u_n\}$ 上升, $\{v_n\}$ 下降, 对所有 n, 我们有

$$u_n<\theta\leqslant\phi<v_n;$$

于是, 对所有 n, 有

$$u_n^{3^n}<\theta^{3^n}\leqslant\phi^{3^n}<v_n^{3^n}.$$

但根据 u_n 和 v_n 的定义, 有

$$u_n^{3^n}=p_n, \quad v_n^{3^n}=p_n+1,$$

所以,

$$p_n<\theta^{3^n}<p_n+1.$$

即 θ^{3^n} 位于两个相继的整数之间. 故对所有 n,

$$[\theta^{3^n}]=p_n$$

是一个素数.

由 θ 的作法我们可知, 对 θ 的认识与对所有素数的认识在本质上是同一回事. 因此, 这个定理也许能给我们一点兴趣, 使我们看到了一个巧妙的想法是如何简洁地实现的, 但是它实际上并没有告诉我们以前我们不知道的任何东西. 只有当我们能用不依赖于所有素数的某种方法来发现 θ 的值时, 这个定理才能显示出它的重要性, 但看来不大可能做到这一点.

习　题

1. 求一个二次多项式 f, 使 $f(0)=2$, $f(1)=3$, $f(2)=5$.
2. 写出一个公式 $y=f(n)$, 使对所有 n, $n=1, 2, \cdots$, y 均为素数.
3. 设 $f(n)=n^2+21n+1$. 证明: 对任一 n, 有 $7\nmid f(n)$, $11\nmid f(n)$.

4. 证明：$n^3+11n+1$ 决不能被 2, 3, 5 或 7 整除.

5. 哪些素数整除 n^2+2?

6. 哪些素数整除 n^2+2n+3?

7. 若 $0<a\leqslant 100$, 且 an^2+n+1 永远不能被 2, 3 或 5 整除, 则 a 可取哪些值?

8. 证明：若对某 n, 奇素数 p 整除 n^2+n+41, 则 $(p+1)^2/4-41$ 是对模 p 的一个二次剩余.

9. 证明：若 p 为素数, 对某 a 和 $n>0$, 有 $p|a^n$, 则对 $k=0, 1, \cdots$, 有 $p|(a+kp)^n$.

10. 若 f 为一多项式, 且 $f(a)=p$ 为素数, 证明对所有 k, 有 $p|f(a+kp)$.

11. 设 $f(n)=\sin\pi((1+(n-1)!)/n)$, 证明：当且仅当 n 为素数时, $f(n)=0$.

12. 设 p_n 表示第 n 个素数, 并令

$$\theta=\sum_{n=1}^{\infty}p_n/10^{n^2}=0.2003000050000007\cdots,$$

证明：
$$p_n=[10^{n^2}\theta]-10^{2n-1}[10^{(n-1)^2}\theta].$$

13. 证明：当且仅当 $n+1$ 不是奇素数时, 前面 n 个正整数之和整除它们的乘积.

14. 证明：一个奇素数可以表为一个以上的相继的正整数之和, 且其表示方式是唯一的.

15. 考虑一张无限的表, 它的前五行为

1 1

1 2 1

1 3 2 3 1

1 4 3 5 2 5 3 4 1

1 5 4 7 3 8 5 7 2 7 5 8 3 7 4 5 1

(a) 此表是怎样造出来的?

(b) 证明第 n 行一共有 $2^{n-1}+1$ 个数, 且它们的和为 $3^{n-1}+1$;

(c) 证明各行中任意两个相邻的数必定互素;

(d) 证明：当且仅当 n 在第 n 行中出现 $n-1$ 次时, n 为素数.

16. 卡塔兰(Catalan, 1876 年)发现, 若 $p_0=2$, $p_{n+1}=2^{p_n}-1$, 则对 $k=1, 2, 3, 4$, p_k 是素数. 也许对所有 k, p_k 都是素数. 这是一个很难解决的猜想, 因为 $\{p_k\}$ 上升得非常快. p_5 大约是几位数?

§22 $\pi(x)$ 的界限

要判定一个具体的大数是不是素数，往往是件困难的工作，但要知道一个给定区间内有多少个素数，我们倒能相当精确地说出. 这和死亡率统计表的概念差不多. 死亡率统计表能够精确地预计下一年度中会有多少72岁的人死去，但它不能将具体的人一个个挑出来. 设 $\pi(x)$ 表示小于或等于 x 的素数个数.（注意，本节中的 x, y, z 将不再局限于取整数值，但其它小写字母仍表示整数，只有 e 是例外，$e=2.7182818284590452\cdots$.）本节的目的是导出 $\pi(x)$ 在 x 很大时的界限. 为此，我们必须用到自然对数函数的某些性质. 若我们用 e 表示 n 无限增大时序列 $\left\{\left(1+\frac{1}{n}\right)^n\right\}$ $(n=1, 2, \cdots)$ 的极限，则对任何 $x>0$，可用

$$x=e^{\log x}$$

来定义 x 的自然对数(记为 $\log x$ 或 $\ln x$). 对任意正数 x, y 和任何 z，自然对数有下列性质:

$$\log xy=\log x+\log y,$$

$$\log x^z=z\log x.$$

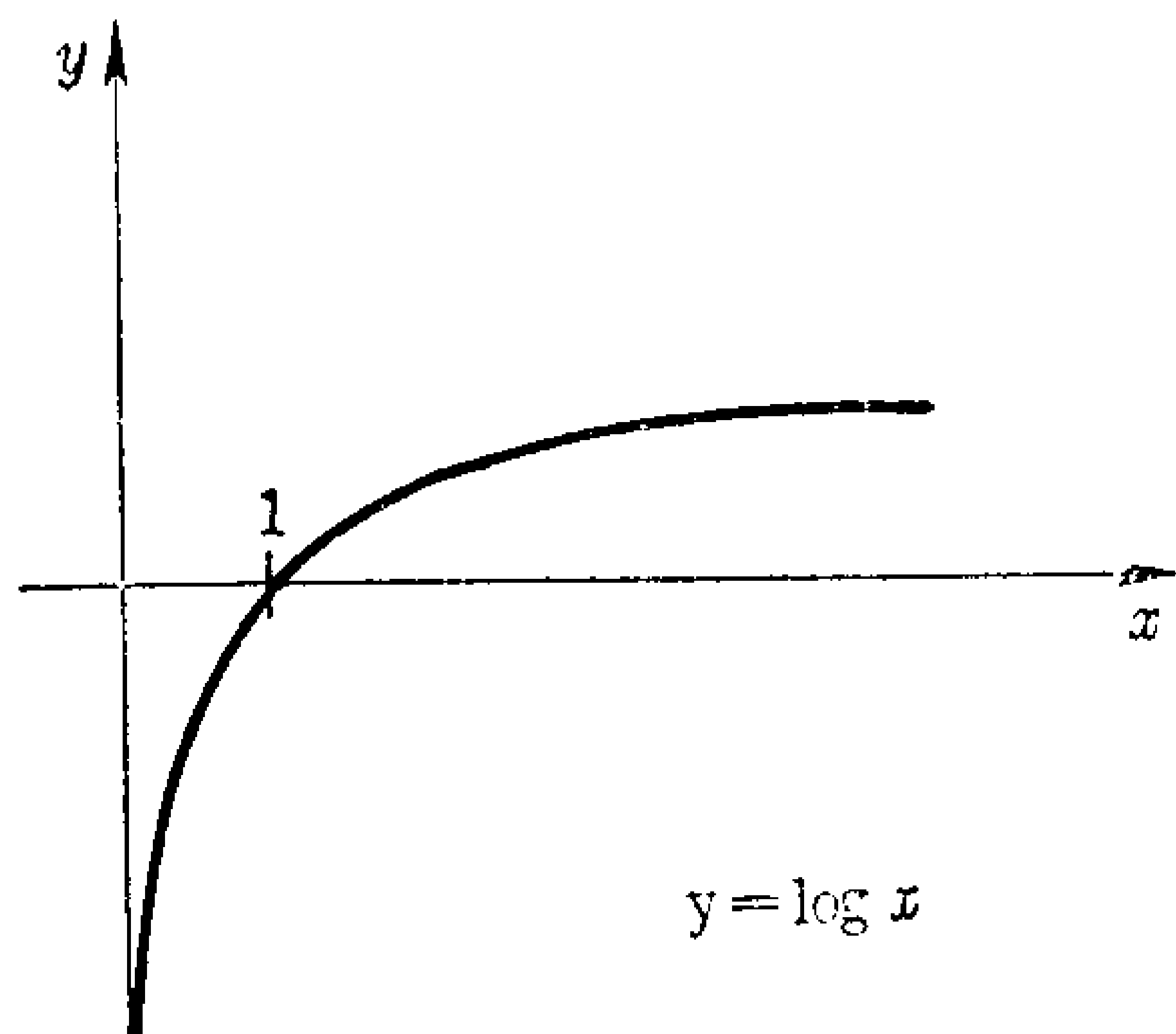
另外还有

$$\lim_{x\to\infty}(\log x)/x=0.$$

x 的自然对数随着 x 增大而增大，但增大的速度逐渐变慢，下图给出了它的部分图形. 它的几个近似值列出如下:

x	0.01	0.1	1	2	3	10	500	1000000
$\log x$	−4.6	−2.3	0	0.7	1.1	2.3	6.2	13.8

除了自然对数的上述性质以外，我们还要不加证明地应用另一结果(引理 6). 利用这些性质和引理 6, 我们将要证明 $\pi(x)$ 的增大速度大致与 $x/\log x$ 相同.



【练习 1】 $\pi(8)$, $\pi(12)$, $\pi(3.2)$, $\pi(\pi)$ 各是多少?

$\pi(x)$ 与 $x/\log x$ 的增大速度大致相同, 这点首先是从数值资料中归纳出来的. 如果你研究一下 $\pi(x)$ 的下列表格:

x	100	200	300	400	500	600	700	800	900	1000
$\pi(x)$	25	46	62	78	95	109	125	139	154	168

x	10,000	100,000	1,000,000	10,000,000	100,000,000
$\pi(x)$	1,229	9,592	78,498	664,579	5,761,455

并计算 $\pi(x)$ 与 $x/\log x$ 之比, 你就会发现这个比停留于 0.9 和 1.2 之间, 且似乎随着 x 的增大而趋近于 1. 本节我们将要证明的是一个较弱的结果:

(1) $$\frac{1}{3}<\frac{\pi(x)\log x}{x}<\frac{10}{3} \quad (\text{当 } x>400,000 \text{ 时}).$$

在开始证明上述结果以前, 我们要提一下已知是成立的更好结果. 事实上,

(2) $$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1,$$

这就是有名的"素数定理". (1)中不等式是由切比雪夫(Tchebyshev)在1850年证得的(他所用的常数比400,000, 1/3, 10/3还要精确些). (2)的历史在1780年就开始了，那时,勒让德猜想,

$$f(x)=\frac{x}{\log x-1.08366}$$

是$\pi(x)$的一个良好的逼近式，他大概也是在与(2)同样的意义上说的,即

$$\lim_{x\to\infty}\pi(x)/f(x)=1.$$

1792年，高斯提出了一个函数，它比勒让德的猜想要更符合实际得多. 1859年，黎曼曾试图证明(2)，他的证明虽不完整，却包含了要求得完整的证明所必需的一些思想. 尽管如此，一直到1896年，阿达玛(Hadamard)和达拉瓦勒布桑(De la Vallée Poussin)才各自独立地证明了素数定理. 今天仍有人在研究如何改进这一定理.

为了证明(1),我们引进一个新函数. 设

$$\theta(x)=\sum_{p\leqslant x}\log p.$$

这一函数似乎没有$\pi(x)=\sum_{p\leqslant x}1$那么自然，但人们发觉它更易于处理. 这两个函数间的关系由引理1给出.

引理1 对所有$x>1$,有

$$\frac{\theta(x)-\theta(x^{1/2})}{\log x}\leqslant\pi(x)-\pi(x^{1/2})\leqslant\frac{2(\theta(x)-\theta(x^{1/2}))}{\log x}.$$

证明 我们有

$$\sum_{x^{1/2}<p\leqslant x}\log x^{1/2}\leqslant\sum_{x^{1/2}<p\leqslant x}\log p\leqslant\sum_{x^{1/2}<p\leqslant x}\log x,$$

即有

(3) $$\frac{1}{2}\log x\sum_{x^{1/2}<p\leqslant x}1\leqslant\sum_{x^{1/2}<p\leqslant x}\log p\leqslant\log x\sum_{x^{1/2}<p\leqslant x}1.$$

但是 $$\sum_{x^{1/2}<p\leqslant x}1=\sum_{p\leqslant x}1-\sum_{p\leqslant x^{1/2}}1=\pi(x)-\pi(x^{1/2}),$$

$$\sum_{x^{1/2}<p\leqslant x}\log p=\theta(x)-\theta(x^{1/2}).$$

因此(3)就成为

$$\frac{1}{2}(\pi(x)-\pi(x^{1/2}))\log x\leqslant\theta(x)-\theta(x^{1/2})$$
$$\leqslant(\pi(x)-\pi(x^{1/2}))\log x,$$

这等价于我们欲证之不等式.

我们以后会看到，与 $\pi(x)$ 相比，$\pi(x^{1/2})$ 可以略而不计，也就是说，

$$\lim_{x\to\infty}\frac{\pi(x^{1/2})}{\pi(x)}=0.$$

$\theta(x^{1/2})$ 与 $\theta(x)$ 相比也是如此. 如果我们将这两项略去，那末引理 1 说明，$\pi(x)$ 与 $\theta(x)/\log x$ 以相同的速度增大. 因此要证明 $\pi(x)$ 增大的速度与 $x/\log x$ 相同，只需证 $\theta(x)$ 增大的速度与 x 相同就行了. 我们还发现，另有一个函数，它看起来比 θ 复杂，但处理起来倒比较方便. 令

(4) $$\psi(x)=\theta(x)+\theta(x^{1/2})+\theta(x^{1/3})+\cdots.$$

可注意到，它的和式只有有限项，这是因为，当 $x^{1/m}<2$ 时，

$$\theta(x^{1/m})=\sum_{p\leqslant x^{1/m}}\log p=0,$$

因为在此和式中已经没有什么项了.

【练习 2】 证明 (4) 中最后一个非零项为 $\theta(x^{1/m})$，其中 $m=[\log x/\log 2]$.

由练习 2 可知，(4) 中和式包含的项数不超过 $2\log x$.

【练习 3】 说明确是这样，即证：$[\log x/\log 2]\leqslant 2\log x$.

【练习 4】(选做) 计算 $\psi(32)$.

现在我们来证一个引理，它将 ψ 和 θ 联系起来. 在某种

意义上说，这一引理也是我们各个引理中最弱的一个，而且你在后面将会看到，这也正是定理1中x为什么要大于400,000的原因.

引理2 对所有$x\geqslant 1$，有

$$\psi(x)-x^{1/2}\log^2 x\leqslant\theta(x)\leqslant\psi(x).$$

证明 首先我们求$\theta(x^{1/m})$的一个上界. 根据定义，

$$\theta(x^{1/m})=\sum_{p\leqslant x^{1/m}}\log p.$$

此和式中最大的一项不大于$\log x^{1/m}$，且此和式至多只有$\pi(x^{1/m})$项. 由于$\pi(x^{1/m})\leqslant x^{1/m}$(因为整数个数至少和素数个数一样多)，我们有

$$\theta(x^{1/m})\leqslant x^{1/m}\log x^{1/m}.$$

将此用于(4)，我们得

$$\psi(x)-\theta(x)=\theta(x^{1/2})+\theta(x^{1/3})+\cdots$$
$$\leqslant x^{1/2}\log x^{1/2}+x^{1/3}\log x^{1/3}+\cdots.$$

上述不等式右端各项都以$x^{1/2}\log x^{1/2}$为上界，且我们已经知道，它们的项数不超过$2\log x$，故有

$$\psi(x)-\theta(x)\leqslant(x^{1/2}\log x^{1/2})2\log x=x^{1/2}\log^2 x,$$

所以，
$$\theta(x)\geqslant\psi(x)-x^{1/2}\log^2 x.$$

又由ψ的定义知，对所有x，有

$$\theta(x)\leqslant\psi(x),$$

这两个不等式并在一起，引理即可得证.

引理2表明，若$\psi(x)$增大的速度与x相同，则$\theta(x)$的增大速度也与x相同. 而我们的目标在于：利用$\psi(x)$造出一个函数，它具有不依赖于素数的形式，于是我们就能相当精确地估计它们增长得多快. 然后将它的增长速度与ψ的增长速度联系起来，再利用引理1和引理2回过头来与π的增长速度

联系起来. 设 $S(x)$ 定义为

(5) $$S(x)=\psi(x)+\psi(x/2)+\psi(x/3)+\cdots.$$

这个函数可以改写成不依赖于素数的形式. 利用(4), 我们可将 $S(x)$ 写为

(6) $$\begin{aligned}S(x)=&\theta(x)+\theta(x^{1/2})+\theta(x^{1/3})+\cdots\\&+\theta(x/2)+\theta((x/2)^{1/2})+\theta((x/2)^{1/3})+\cdots\\&+\theta(x/3)+\theta((x/3)^{1/2})+\theta((x/3)^{1/3})+\cdots.\end{aligned}$$

注意, (5) 和 (6) 中的和式均只有有限项, 每一行和式中必有这样一项, 在这一项以后, 函数的自变量很小, 以至于相应的函数值都为零.

【练习 5】(选做) (6) 的右端大约有多少非零项?

你可能会想到(也应该想到): "会有人想到要考虑象 $S(x)$ 这样一个函数吗?" 切比雪夫就考虑了这个函数. 而且, 要是你有切比雪夫的才华, 又曾在相当长的时间里孜孜不倦地而又富于想象地研究过 $\psi(x)$ 的估值问题, 那么你也很可能会想到去考虑这一和式的. 这的确是件相当自然的事, 人们后来的认识就无可辩驳地说明了这一点.

【练习 6】 (6) 中第二行最后一个非零项是什么? 第二列中最后一个非零项是什么?

我们现在来算一算 $\log p$ 在 (6) 的右端一共出现了多少次. 首先看一看它在第一列中出现了几次: 当且仅当 $p\leqslant x/m$ 时, $\log p$ 出现在 $\theta(x/m)$ 的和式中. 也就是说, 若 m 的值满足 $m\leqslant x/p$, $\log p$ 就在 $\theta(x/m)$ 的和式中出现. 这种整数一共有 $[x/p]$ 个. 在第二列中, 当且仅当 $p\leqslant(x/m)^{1/2}$, 也即当且仅当 $m\leqslant x/p^2$ 时, $\log p$ 在 $\theta((x/m)^{1/2})$ 的和式中出现. 因此, 当 $m=1, 2, \cdots, [x/p^2]$ 时, 在 $\theta((x/m)^{1/2})$ 中就有 $\log p$ 出现. 用同样的方法可证, $\log p$ 在 (6) 的第三列中出现 $[x/p^3]$

次．如此继续，我们就证明了：

引理3 在$S(x)$的和式中，$\log p$刚好出现$S_p(x)$次，这里的$S_p(x)$为

$$S_p(x)=[x/p]+[x/p^2]+[x/p^3]+\cdots.$$

【练习7】 这也是一个有限和吗？

【练习8】（选做） 证明：

$$\sum_{m\leqslant x}\theta(x/m)=\sum_{p\leqslant x}[x/p]\log p.$$

引理4 能整除$n!$的p的最高次幂为$S_p(n)$.

证明 p的每个倍数，只要小于或等于n，都为$n!$增加p的一个幂次，这种倍数一共有$[n/p]$个；p^2的每个倍数也为$n!$提供了p的一个新的幂次，这种倍数一共有$[n/p^2]$个；如此类推，p^k的倍数提供的p的幂次一共有$[n/p^k]$个．因此，以

$$[n/p]+[n/p^2]+[n/p^3]+\cdots$$

为指数的p的乘幂恰好整除$n!$.

【练习9】（选做） 引理4中的和式到底有多少项？

【练习10】 1111！中含有多少个因子11？

【练习11】 证明：$[x/n]=[[x]/n]$.

借助于引理4，我们可将$S(x)$改写成不明显地涉及到任何素数的形式．

引理5 对所有$x\geqslant1$,

$$S(x)=\sum_{n\leqslant x}\log n.$$

可以认为，此引理是估计$\pi(x)$的关键的一步．在证明这一引理后，我们就要求出$S(x)$的增长速度，但这不过是一件普通的事而已．这件事也做好以后，我们就要回过来再将$S(x)$与$\pi(x)$联系起来，而这也同样是一件普通的事．

引理 5 的证明 由(6)我们知，$S(x)$ 是一些形为 $\log p$ 的项的一个和式，由引理 3 可知 $\log p$ 在此和式中出现的次数正好是 $S_p(x)$ 次，因此，

(7) $$S(x)=S_2(x)\log 2+S_3(x)\log 3+S_5(x)\log 5+\cdots$$
$$=\log\left(2^{S_2(x)}3^{S_3(x)}5^{S_5(x)}\cdots\right).$$

另一方面，

(8) $$[x]!=2^{e_2(x)}3^{e_3(x)}5^{e_5(x)}\cdots,$$

这里，根据引理 4，

$$e_p(x)=[[x]/p]+[[x]/p^2]+[[x]/p^3]+\cdots.$$

但由练习 11，对任何 p 和 k 有，$[[x]/p^k]=[x/p^k]$，故知 $e_p(x)=S_p(x)$. 有了这一点，我们比较(7)和(8)可知，

$$S(x)=\log[x]!=\sum_{1\leqslant n\leqslant[x]}\log n=\sum_{n\leqslant x}\log n,$$

引理得证.

【练习 12】(选做) 对 x 的某几个值近似地算出 $S(x)$，并估计它的增长率.

为了发现 $S(x)$ 增长得多快，我们需要数学分析中的一个结果，这一结果我们将加以承认而不予证明.

引理 6 对任何整数 n, $n\geqslant 7$, 有

$$\left(\frac{n}{e}\right)^n\leqslant n!\leqslant n\left(\frac{n}{e}\right)^n.$$

这一引理给出的是一个有名的结果 (Stirling 公式) 的一种较弱的形式. 如果你记得自然对数的底 e 的定义，就可用归纳法证明这一引理. 由此引理可得

引理 7 对任何整数 n, $n\geqslant 7$, 有

$$n\log n-n\leqslant S(n)\leqslant n\log n-n+\log n.$$

证明 由于

$$S(n)=\sum_{k\leqslant n}\log k=\log n!,$$

由引理 6, 我们有

$$S(n) \leqslant \log n\left(\frac{n}{e}\right)^n = \log n + n(\log n - \log e)$$

$$= n\log n - n + \log n,$$

$$S(n) \geqslant \log\left(\frac{n}{e}\right)^n = n\log n - n.$$

引理 7 说明，当 x 为整数时，$S(x)$ 的特性大致上有点象 $x\log x$. 即使 x 不是整数，这也是正确的. 我们用普通的计算还可证得:

引理 8 对任何 x, $x>7$, 有

$$x\log x - x - \log x - 1 \leqslant S(x) \leqslant x\log x - x + \log x.$$

我们略去详细的论证,因为证明起来较为乏味. 引理 8 说明，$S(x)$ 与 $x\log x$ 以同样的速率增长. 现在我们要证，$\psi(x)$ 与 x 也以同样的速率增长. 我们需要进行更多的计算,而作为开始,我们要用到另一种巧妙的想法,它是我们从切比雪夫那里学来的. 考虑 $S(x)-2S(x/2)$，根据 $S(x)$ 的定义，我们有

(9) $$S(x)-2S(x/2) = \psi(x)-\psi(x/2)+\psi(x/3)-\psi(x/4)+\cdots.$$

根据引理 8，我们可得 $S(x)-2S(x/2)$ 的上下界: 当 $x>7$ 时，

$$S(x)-2S(x/2) \leqslant x\log x - x + \log x - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2} - \log\frac{x}{2} - 1\right)$$

$$= x\log 2 + 3\log x + 2 - 2\log 2.$$

在另一方向上，我们有

$$S(x)-2S(x/2) \geqslant x\log x - x - \log x - 1 - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2} + \log\frac{x}{2}\right)$$

$$= x\log 2 - 3\log x + 2\log 2 - 1.$$

我们将这两个不等式合并在下列引理中.

引理 9 对 $x>7$, 有

$$x\log 2-3\log x+2\log 2-1\leqslant S(x)-2S(x/2)$$
$$\leqslant x\log 2+3\log x+2-2\log 2.$$

我们的事就要做完了. 注意, 当 x 减小时, $\psi(x)$ 并不增大, 这是因为,

$$\psi(x)=\theta(x)+\theta(x^{1/2})+\theta(x^{1/3})+\cdots,$$

而当 x 减小时, 对任一 m, $\theta(x^{1/m})$ 都不增大. 因此,

$$S(x)-2S(x/2)=\psi(x)-\psi(x/2)+\psi(x/3)-\cdots$$

是一个逐项非增的交错级数, 故它写成下列形式时:

$$S(x)-2S(x/2)=\psi(x)-(\psi(x/2)-\psi(x/3))$$
$$-(\psi(x/4)-\psi(x/5))-\cdots$$

就表明 $$S(x)-2S(x/2)\leqslant\psi(x);$$

又如级数写成下列形式时:

$$S(x)-2S(x/2)=(\psi(x)-\psi(x/2))$$
$$+(\psi(x/3)-\psi(x/4))+\cdots$$

就表明 $$S(x)-2S(x/2)\geqslant\psi(x)-\psi(x/2).$$

因此, 我们有

(10) $$\psi(x)-\psi(x/2)\leqslant S(x)-2S(x/2)\leqslant\psi(x).$$

(10) 中右边的不等式为 $\psi(x)$ 给出了一个下界. 而由引理 9, 我们有

$$\psi(x)\geqslant S(x)-2S(x/2)\geqslant x\log 2-3\log x+2\log 2-1.$$

由此我们可得下列结论:

引理 10 当 $x>150$ 时, $\psi(x)\geqslant x/2$.

证明 显然, 当 $x\to\infty$ 时, $(3\log x-2\log 2+1)/x$ 下降并趋于零. 若 $x>150$, 则由于 $e^5=148.4\cdots<150$, 必有

$$\frac{3\log x-2\log 2+1}{x}\leqslant\frac{3\cdot 5-1\cdot 4+1}{150}\leqslant 0.1.$$

故当 $x>150$ 时,

$$x\log 2-3\log x+2\log 2-1\geqslant x(\log 2-0.1)\geqslant x/2.$$

又,显然, 对于充分大的 x, 可以证明对任意 $\varepsilon>0$, 有 $\psi(x)\geqslant x(\log 2-\varepsilon)$. 这是毫无困难的, 因为从素数定理推知, 当 $x\to\infty$ 时, $\psi(x)/x\to 1$. 这样, 当 x 充分大时, 对任一 $\varepsilon>0$, 成立 $\psi(x)\geqslant x(1-\varepsilon)$.

欲求 ψ 的一个上界, 我们需要一个更为巧妙的办法, 它包含在以下两个引理中.

引理 11 对 $x>403$, 有 $\psi(x)-\psi(x/2)\leqslant 3x/4$.

证明 由(10)和引理 9, 我们得

$$\begin{aligned}\psi(x)-\psi(x/2)&\leqslant S(x)-2S(x/2)\\&\leqslant x\log 2+3\log x+2-2\log 2.\end{aligned}$$

显然, 当 $x\to\infty$时, $(3\log x+2-2\log 2)/x$ 下降并趋于零. 若 $x>403$(选取此数是由于 $e^6=403.4\cdots$), 则此分数至多是

$$\frac{18+2-1.4}{403}<0.05.$$

因此, 对 $x>403$, 我们有

$$x\log 2+3\log x+2-2\log 2<x(0.694+0.05)<3x/4,$$

引理得证.

有了引理 11, 我们就能证明下列引理:

引理 12 若 $x>403$, 则 $\psi(x)\leqslant 3x/2$.

证明 由引理 11, 我们得

$$\psi(x)-\frac{3x}{2}\leqslant\psi(x/2)-\frac{3x}{4}.$$

若重复应用此式, 则对任一整数 n, 我们有

$$\psi(x)-\frac{3x}{2}\leqslant\psi(x/2)-\frac{3x}{4}\leqslant\psi(x/8)-\frac{3x}{16}$$

$$\leqslant\cdots\leqslant\psi(x/2^n)-\frac{3x}{2^{n+1}}.$$

n 为充分大时，必有 $\psi(x/2^n)=0$.

【练习 13】(选做) “充分大”是指多大？

对于这个充分大的 n，我们就有

$$\psi(x)-\frac{3x}{2}\leqslant-\frac{3x}{2^{n+1}}\leqslant 0,$$

引理得证.

最后，我们可证

定理 1 若 $x>400,000$，则有

$$\frac{1}{3}\frac{x}{\log x}\leqslant\pi(x)\leqslant\frac{10}{3}\frac{x}{\log x}.$$

证明 我们有

$$\theta(x)=\sum_{p\leqslant x}\log p\geqslant\sum_{x^{1/2}<p\leqslant x}\log p.$$

最后这一和式中共有 $\pi(x)-\pi(x^{1/2})$ 项，且最小的一项不小于 $\log x^{1/2}$，因此，

$$\theta(x)\geqslant(\pi(x)-\pi(x^{1/2}))\log x^{1/2}\geqslant(\pi(x)-x^{1/2})\log x^{1/2},$$

即
$$\pi(x)-x^{1/2}\leqslant\frac{2\theta(x)}{\log x}.$$

由 ψ 的定义，我们知 $\psi(x)\geqslant\theta(x)$，故有

$$\pi(x)\leqslant\frac{2\psi(x)}{\log x}+x^{1/2}.$$

应用引理 12，我们得，对 $x>403$，有

$$\pi(x)\leqslant\frac{2}{\log x}\cdot\frac{3x}{2}+x^{1/2}.$$

此外，容易看出，当 $x>400,000$ 时，有

$$x^{1/2}<\frac{0.01x}{\log x}.$$

【练习 14】(选做)　验证这一点.

于是,我们知,当 $x>400,000$ 时,

$$\pi(x)\leqslant\frac{3x}{\log x}+\frac{0.01x}{\log x}<\frac{10}{3}\frac{x}{\log x}.$$

这就证明了定理的一半. 为了证明定理的另一半,我们有

$$\theta(x)=\sum_{p\leqslant x}\log p\leqslant\log x\sum_{p\leqslant x}1=\pi(x)\log x.$$

应用此式以及引理 2 和引理 10, 我们有

$$\pi(x)\geqslant\frac{\theta(x)}{\log x}\geqslant\frac{\psi(x)-x^{1/2}\log^2 x}{\log x}\geqslant\frac{1}{2}\frac{x}{\log x}-x^{1/2}\log x.$$

【练习 15】(选做)　验证:当 $x>400,000$ 时, $(\log^2 x)/x^{1/2}<0.15$.

由练习 15, 我们得,当 $x>400,000$ 时,

$$\pi(x)\geqslant\frac{1}{2}\frac{x}{\log x}-0.15\frac{x}{\log x}\geqslant\frac{1}{3}\frac{x}{\log x},$$

于是定理得证.

在估计常数时,本来我们还可以做得更为精确些. 对切比雪夫的方法稍作修饰,就可以证明,对充分大的 x, 有

$$\frac{0.95695x}{\log x}\leqslant\pi(x)\leqslant\frac{1.04423x}{\log x}.$$

而且,对 $x>400,000$, 还知道有

$$\frac{0.96x}{\log x}\leqslant\pi(x)\leqslant\frac{1.12x}{\log x}.$$

但是,以上两式都比不上素数定理的下列说法:

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1.$$

习　　题

1. 设 p_n 表示第 n 个素数.

   (a) 说明: $\pi(p_n)=n$;

   (b) 说明: 若 $n>400,000$, 则 $p_n>400,000$;

   (c) 证明: 若 $n>400,000$, 则有

$$\frac{3n}{10}\leqslant\frac{p_n}{\log p_n}\leqslant 3n;$$

   (d) 证明: 若 $n>400,000$, 则 $\pi(n^2)>n$;

   (e) 设 $x_n=p_n/n$, 证明: 若 $n>400,000$, 则 $1<x_n<n$;

   (f) 证明: 若 $n>400,000$, 则有

$$\frac{3}{10}\leqslant\frac{x_n}{\log nx_n}\leqslant 3;$$

   (g) 证明: 若 $n>400,000$, 则有

$$\frac{3}{10}n\log n\leqslant p_n\leqslant 6n\log n;$$

   因此, p_n 与 $n\log n$ 以大致相同的速率增大.

2. 利用上题中的(g), 证明下列级数发散:

$$\sum_{n=1}^{\infty}1/p_n.$$

3. 利用题 1 中的(c), 求下式的增长率:

$$\sum_{n=1}^{N}(\log p_n)/p_n.$$

4. (a) 证明: 当 x 增大时, 下列函数递减:

$$\frac{(x+1)\log(x+1)}{x\log x};$$

   (b) 由(a)推证: 对 $n>400,000$, 有

$$(n+1)\log(n+1)\leqslant\frac{21}{20}n\log n;$$

   (c) 根据(b)和题(1)之(g), 证明: 对充分大的 n, 有

$$p_{n+1}<21p_n.$$

   (事实上, 对一切 n, 成立 $p_{n+1}<2p_n$.)

5. (a) 说明: 对任一 n 和每一素数 p, 存在唯一的一个整数 r_p, 使

$$p^{r_p} \leqslant 2n < p^{r_p+1};$$

(b) 能整除整数 1, 2, …, 2n 中某一数的 p 的最大乘幂的次数是多少?

(c) 证明:

$$M(2n) = \prod_{p<2n} p^{r_p} \mid (2n)!;$$

(d) 证明: $\psi(2n) = \log M(2n)$;

(e) 证明: 整除 $\binom{2n}{n}$ 的 p 的最大乘幂的次数为

$$\sum_{m=1}^{r_p} ([2n/p^m] - 2[n/p^m]);$$

(f) 由(e)推证: $\binom{2n}{n} \bigg| M(2n)$;

(g) 证明: $\binom{2n}{n} \geqslant 2^n$;

(h) 根据(f)和(g)推证: $M(2n) \geqslant 2^n$;

(i) 根据(d)和(h)推证: $\psi(2n) \geqslant n \log 2$;

(j) 根据(i)推证: 对 $x>40$, 有 $\psi(x) > x/3$. (或者推证与此类似但系数不同的某一关系式.)

§23 杂　　题

1．证明：对 $n\geqslant1$，$(2^n+(-1)^{n+1})/3$ 是奇数．

2．某人用 5 元钱买了一些邮票，有六分、五分和一角三种，五分邮票数是六分邮票数的 1/4，每一种邮票他各买了多少张？

3．1494 年，有人称，134217727 是素数．这数为 $2^{27}-1$，证明此人说错了．

4．若 p 和 q 均为大于或等于 5 的素数，证明 $24\mid(p^2-q^2)$．

5．(a) 一个平方数对模 9 可以与哪些数同余？

(b) 314,159,267,144 是一个平方数吗？

6．设 a' 表示 $ax\equiv1(\mathrm{mod}\ p)$ 的解，$a=1, 2, \cdots, p-1$．

(a) 证明：$(ab)'\equiv a'b'(\mathrm{mod}\ p)$；

(b) 证明 $(a+b)'\equiv a'+b'(\mathrm{mod}\ p)$ 未必成立．

7．利用表 A 求出最小的六个相继的奇合数．

8．证明：若对某两整数 r 和 s，有

$$a=r^2-2rs-s^2,$$
$$b=r^2+s^2$$
$$c=r^2+2rs-s^2,$$

则 a^2，b^2，c^2 构成等差级数．

9．帕斯卡(Pascal)有一次写道，他已发现，任何相继的两个整数的立方差减 1 与小于或等于其中较小的一数的所有正整数之和的 6 倍相等．证明他是正确的．

10．若 a 和 b 为奇数，证明 $64\mid(a^2-1)(b^2-1)$．

11．由下列各式推出一个定理：

$$3^2+4^2=5^2,$$
$$10^2+11^2+12^2=13^2+14^2,$$
$$21^2+22^2+23^2+24^2=25^2+26^2+27^2,$$
$$36^2+37^2+38^2+39^2+40^2=41^2+42^2+43^2+44^2.$$

12．一个数从左读向右或从右读向左得出同一数，称为回文数，如 3141413.

(a) 有多少个两位数是回文数？

(b) 有多少个三位数是回文数？

(c) 有多少个 k 位数是回文数？

13．令 (a, b, c) 表示 a, b, c 三数之最大公因子.

(a) 证明：$(a, b, c)=((a, b), c)$；

(b) 若 $(a, b)=(b, c)=(c, a)=1$，证明 $(a, b, c)=1$；

(c) (b)之逆命理是否成立？

14．对哪些正整数 k，下列方程有解？

$$kx\equiv 1 (\bmod k(k+1)/2).$$

15．若 $p\geqslant 5$ 为素数，证明 p^2+2 是合数.

16．下列问题至少有 400 年的历史了：一队男人、妇女和儿童，总计 20 人．他们一共拿出了 20 元钱，男人每人拿出 3 元，妇女每人拿出 2 元，儿童每人拿出 0.50 元，问队中男人、妇女和儿童各有多少人？

17．若 a 和 b 为正整数，当且仅当：对于素数 p，$p|a$ 蕴涵 $p|b$，我们称 a 弱整除 b（或称 a 是 b 的一个弱因子），并记作 $a\int b$.

(a) 举几个整数 a 和 b 的例，它们满足 $a>b$，且 $a\int b$；

(b) 证明：若 $a|b$，必有 $a\int b$；

(c) 证明：若 $a\int 1$，必有 $a=1$；

(d) 证明：若 $a\int b$, $b\int c$, 则 $a\int c$;

(e) 证明：若 $a\int b$, 则对所有正整数 c, 有 $ac\int bc$;

(f) 证明：若 $a\int b$, $c\int d$, 则 $ac\int bd$;

(g) 证明：若 $ab\int c$, 则 $a\int c$, $b\int c$;

(h) 证明：若 $ac\int bc$, 且 $(a, c)\int(b, c)$, 则 $a\int b$;

(i) 证明：若 $ac\int bc$, 且 $(a, c)=1$, 则 $a\int b$;

(j) 证明：若 $a\int b$, 则对所有正整数 c, 有 $(a, c)\int(b, c)$;

(k) 证明：若 $a\int b$, $c\int d$, 则 $(a, c)\int(b, d)$;

(l) 证明：若 $a\int b$, 则对所有正整数 m 和 n, 有 $a^n\int b^m$;

(m) 证明：若存在整数 m 和 n 使 $a^n\int b^m$, 则 $a\int b$;

(n) 证明：若 $a\int c$, $b\int c$, 则 $ab\int c$;

(o) (c)到(n)中，哪些性质对正整数的普通整除性不成立？举几个例子.

18. 作出 f 的一个公式，使 n 为偶数时，$f(n)$ 是 $1/2$, n 为奇数时，$f(n)$ 为 1.

19. 求具有下列性质的最小正整数 n:

$$2|n,\ 3|(n+1),\ 5|(n+2),\ 7|(n+3),$$
$$11|(n+4),\ 13|(n+5).$$

若再加上条件 $17|(n+6)$, 则这样的 n 又是什么数?

20. 证明：若 $n=a^2+b^2=c^2+d^2$, 则

$$n=\frac{((a-c)^2+(b-d)^2)((a+c)^2+(b-d)^2)}{4(b-d)^2}.$$

因此，若 n 可用两种不同的方式写为两个平方数的和，则 n 是合数.

21. 利用题 20 的结果，分解因子：

(a) $533=23^2+2^2=22^2+7^2$;

(b) $1073=32^2+7^2=28^2+17^2$.

22. 利用表 B 和题 20，分解因子：(a) 170,833；(b) 182,410.

23. 证明：若 $a+b$ 为偶数，则 $24|ab(a^2-b^2)$.

24. 若 $n=a^2+b^2+c^2$，其中 a, b, c 均为非负数，证明

$$(n/3)^{1/2}\leqslant \max(a, b, c)\leqslant n^{1/2}.$$

25. 高斯曾证明，若 $m=2^a n$，其中 a 为整数，$n=1$ 或者 n 是形为 2^k+1 的不同的素数的乘积，则用圆规和直尺可作出正 m 边形. 列出能用圆规和直尺作出的边数在 40 以下的所有正多边形.

26. $1^2+2^2=3^2-2^2$, $2^2+3^2=7^2-6^2$, $3^2+4^2=13^2-12^2$, $4^2+5^2=21^2-20^2$. 一般地能有什么结果?

27. 已知对任一 $k\geqslant 0$, $8k+3=x^2+y^2+z^2$ 有解.

(a) 证明 x, y, z 均为奇数;

(b) 推证 k 等于三个三角形数之和.

28. $(1/3)^2+(2/3)=(1/3)+(2/3)^2$; 你对此感到惊奇吗?

29. (a) 求 $x^4+y^4=z^4$ 的满足 $xyz\neq 0$ 的实数解;

(b) 已知 $x^4+y^4=z^4$ 没有整数解，证明它也没有有理数解.

30. 验证：$(5+5/24)^{1/2}=5(5/24)^{1/2}$，还有没有其它与此相似的数呢?

31. 证明：

(a) 若 $a|c$, $b|c$, 且 $(a, b)=d$, 则 $ab|cd$;

(b) 若 $(a, c)=1$, $(b, c)=d$, 则 $(ab, c)=d$.

32. 0.123456789101112131415…是有理数吗?

33. (a) 设 n 是以 12 为基写出的一个整数，m 是 n 的倒写数（即将 n 的各位数字的次序颠倒写出来的数），证明 $\varepsilon|(n-m)$;

(b) 将此推广到以任意数 b 为基的情况.

34. (a) 假定$0\leqslant m<121$，若$210n+m$是素数，证明m也是素数；

(b) 将此推广，即证：如$P_k=p_1p_2\cdots p_k$（p_i表示第i个素数），且$0\leqslant m<p_{k+1}^2$，则当P_kn+m为素数时，m也是素数.

35. (a) 求使$3p+1$为平方数的所有素数p；

(b) 求使$3p+2$为平方数的所有素数p.

36. 有一次，费马在给某人的信中写道："请你证明一个命题.此命题我虽然相信是正确的，但我得老实承认，我还不能证明它：若a, b为整数，且

(1) $$a^2+b^2=2(a+b)x+x^2,$$

则x和x^2均为无理数."证明：除非$a=b=0$，否则任何整数x都不能满足方程(1).

37. 应用有理数根的定理完成题36中有关结论的证明.也即证明：若(1)没有整数根，则它也没有有理数根.对a和b加什么限制后，还可保证x^2为无理数？

38. 若$n=(6m+1)(12m+1)(18m+1)$，证明$n-1$可为$36m$整除.

39. 好多年前的今天，某人借了若干元钱，其数目正好是整数，利息按普通的单利计算(即每年的利息不计入下一年的本金). 今天，他用204.13元还清了这笔债，问他何时借了这笔钱？借的数目是多少？利率是多少？

40. (a) 证明：若n是一个合数，则$111\cdots11$(有n位，全为1)也是合数；

(b) 它的逆命题成立吗？

41. 证明：若$a|c$, $c|b$, $(a, b)=1$，则$a=\pm1$.

42. $2+1$, $2\cdot3+1$, $2\cdot3\cdot5+1$, $2\cdot3\cdot5\cdot7+1$, $\cdots$，这些数中，哪

些可写为两个平方数的和?

43. 若 n 是一个偶完全数，$n\neq 6$，证明它的十二进位数表示式中的最后一位是 4.

44. 设 $f(x)$ 在 $x\geqslant 0$ 时非负且单调非降，当且仅当对所有正整数 m 和 n 有 $f(nm)\geqslant f(n)f(m)$ 时，我们称 f 是"略有积性"的.

(a) 证明: $f(n)=n^k$ (其中 k 为正整数) 是略有积性的;

(b) 证明: 两个略有积性的函数之积也是略有积性的;

(c) 证明: 若 $g(x)$ 对 $x\geqslant 0$ 是一个单调非降函数，则 $n^{g(n)}$ 是略有积性的.

45. 设 $f(n)$ 表示 n 的正的奇因子个数.

(a) 对 $n=2, 3, 4, \cdots, 15$，列出 f 的值;

(b) 证明: $f(2^n p^m)=m+1$ (p 为奇素数);

(c) 为 $f(2^n p_1^{e_1} p_2^{e_2}\cdots p_k^{e_k})$ 猜想一个公式(各 p_i 全为奇素数);

(d) 对 k 用归纳法证明此公式成立.

46. 证明: 对 $n=1, 2, \cdots$，有

$$2!4!\cdots(2n)!\geqslant((n+1)!)^n.$$

47. (a) 证明: 若 $(a, b)=(a, c)=1$，则 $(a, bc)=1$;

(b) 证明: 若 $(a, b)=1$，则对任意正整数 m 和 n，有 $(a^n, b^m)=1$.

48. 证明: 各孪生素数之和 $2p+2$ (即 p 和 $p+2$ 均为素数) 在 $p>3$ 时能被 12 整除.

49. 若 $p\mid(ra-b)$，$p\mid(rc-d)$，证明 $p\mid(ad-bc)$.

50. 若 $d>0$，$d\mid n$，且 $(d, n/d)=1$，则 d 称为 n 的一个"幺因子".

(a) 120 有哪些幺因子? 360 有哪些幺因子?

(b) 哪些整数的所有因子全为幺因子？

(c) 若 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$，$n$ 有多少个幺因子？

(d) 若 $\sum d=2n$（这里求和是对 n 的各个幺因子 d 进行的），则 n 称为"幺完全数"．找出两个幺完全数．

51. 证明：任一 $n>0$ 至少满足下列各同余式之一：

$n\equiv 0 \pmod 2$，$n\equiv 0 \pmod 3$，$n\equiv 1 \pmod 4$，

$n\equiv 3 \pmod 8$，$n\equiv 7 \pmod{12}$，$n\equiv 23 \pmod{24}$．

52. 证明 9^{9^9} 的最后两位数为 89．

53. 若 p 为素数，$ap+b=c^2$，证明：使 $kp+b$ 为平方数的 k 值由 $k=pn^2\pm 2cn+a$ 给出，其中 n 为任意整数．

54. 若 $m>1$ 为奇数，证明 2^m+1 是合数．

55. 用归纳法证明 $3^{n+2} \mid (10^{3^n}-1)$，$n=0, 1, 2, \cdots$．

56. 若每个小于或等于 n 的正整数均为 n 的不同因子之和，我们就称 n 是"实用数"．

(a) 证明 12 是一个实用数；

(b) 证明 10 不是实用数；

(c) 找出一个大于 12 的实用数；

(d) 证明 2 的各次乘幂均为实用数；

(e) 证明每个偶完全数均为实用数．

57. 证明 $x^6+2^6=z^6$ 没有满足 $(x, z)=1$ 的解．

58. (a) 证明：若对某 n 有 $p \mid (n^2+2an+b)$，则 $((a^2-b)/p)=1$；

(b) 哪些素数能整除 n^2+2n+2？

59. 假定 a, b, c 三数没有大于 1 的公因子，且满足下列方程：

$$ab(a+b)(a-b)=c^2.$$

(a) 证明：a 和 b 均为奇数；

(b) 证明：a，b，$(a+b)/2$，$(a-b)/2$ 四数两两互素；

(c) 推证：a，b，$(a+b)/2$，$(a-b)/2$ 四数都是平方数；

(d) 令 $(a+b)/2=r^2$，$(a-b)/2=s^2$，用 r 和 s 表出 a 和 b；

(e) 推证：若 $ab(a^2-b^2)=c^2$ 有解，且 a，b，c 没有大于 1 的公因子，则下列方程也有非零解：

$$r^2+s^2=t^2,$$
$$r^2-s^2=u^2.$$

60．证明有无限多个三角形数也是平方数．找出四个这样的平方数．

61．证明：每个正整数均可写为

$$n=x^2+y^2-z^2,$$

其中 x，y，z 为整数．

62．设 $\langle x\rangle$ 表示 x 的小数部分，即 $\langle x\rangle=x-[x]$．

(a) 证明：若 $(a, n)=1$，则下列各数：

$$\langle a/n\rangle,\ \langle 2a/n\rangle,\ \cdots,\ \langle (n-1)a/n\rangle$$

是如下一组数的一个排列：

$$1/n,\ 2/n,\ \cdots,\ (n-1)/n;$$

(b) 证明：若 $(a, n)=1$，则

$$\sum_{k=0}^{n-1}\left[\frac{ak}{n}\right]=\frac{(a-1)(n-1)}{2}.$$

63．说明：并非每一正整数 n 均可写为 $n=x^2-y^2$，其中 x 和 y 为整数．

64．证明下列方程没有非平凡解：

$$x^3+y^3+z^3+x^2y+y^2z+z^2x+xyz=0.$$

65．求 m 和 n，使下列各个最大公因子都大于 1：

$$(m, n),\ (m+1, n),\ (m, n+1),\ (m+1, n+1).$$

66．(a) 证明：不可能成立 $n^2+(n+1)^2+(n+2)^2=m^2$；

(b) 证明：当 $1^2+2^2+\cdots+k^2$ 是一个二次非剩余 $(\mathrm{mod}(k+1))$时，不可能成立 $n^2+(n+1)^2+\cdots+(n+k)^2=m^2$；

(c) 开头三个这样的 k 值是什么？

67. 证明：当 $n>1$ 时，$n!$ 的最后一位非零数字是偶数.

68. 证明：2 的任何次乘幂都不是两个或两个以上相继正整数的和.

69. 设 $f(n)$ 表示满足 $m!\equiv 0(\mathrm{mod}\, n)$ 的最小正整数 m.

(a) 对 $n=2, 3, \cdots, 20$, 列出 f 的值；

(b) 证明：$f(p)=p$；

(c) 证明：若 p 和 q 为不同的素数，则 $f(pq)=\max(p, q)$；

(d) 证明：若 $p>k$，则 $f(p^k)=kp$.

70. 证明：当 $n>3$ 时，$\sum_{k=1}^{n} k!$ 都不是平方数.

71. 找出构成算术级数的九个整数，使它们的平方和仍是一个平方数.

72. (a) 被 9 整除且各位数字互不相同的最大的一个十位数是什么？

(b) 被 9 整除且各位数字互不相同的最大的一个八位数是什么？

(c) 被 11 整除且各位数字分别为 1, 2, 3, 4 的最大一个四位数是什么？

(d) 被 11 整除且各位数字分别为 1, 2, $\cdots$, 9 的最大一个九位数是什么？

73. 若 n 为合数，证明 $\phi(n)\leqslant n-n^{1/2}$.

74. 已知 n，问 $n=xy$ 且 $(x, y)=1$ 有多少组解？

75. 将正整数螺旋式地写入下表中:

17	16	15	14	13
18	5	4	3	12
19	6	1	2	11
20	7	8	9	10
21	22	23	…	

若 1 位于直角坐标系的原点, $n\geqslant 0$, 那么,

(a) 在 $(n, 0)$ 处的整数是什么数?

(b) 在 (n, n) 处的整数是什么数?

(c) 在 $(-n, 0)$ 处的整数是什么数?

(d) $(2n+1)^2$ 位于何处?

(e) $(2n)^2$ 位于何处?

(f) 1000 位于何处?

76. 若 p 为素数,证明:当且仅当下式成立时, $p+2$ 也为素数:

$$4((p-1)!+1)+p\equiv 0(\mathrm{mod}(p+2)).$$

77. (a) 已知 $n>0$, 证明: 存在一个整数 m, 使

$$((n+1)^{1/2}+n^{1/2})^2=(m+1)^{1/2}+m^{1/2};$$

(b) 你总能找到一个 m 使下式成立吗?

$$((n+1)^{1/2}+n^{1/2})^3=(m+1)^{1/2}+m^{1/2}.$$

78. 设 $(m, n)=1$, 将小于或等于 n 且与 n 互素的 $\phi(n)$ 个数与小于或等于 m 且与 m 互素的 $\phi(m)$ 个数相乘, 所得的乘积给出了小于或等于 mn 且与 mn 互素的 $\phi(mn)$ 个数. 这一说法对不对?

79. 若 $(a, m)=1$, 则 $a, 2a, \cdots, ma$ 的最小剩余 $(\mathrm{mod}\ m)$ 是 $1, 2, \cdots, m$ 的一个排列. 那么, 要是 $(a, m)\neq 1$, 又怎么样呢?

80. 设 p_i 表示第 i 个素数. 证明 $P_n=p_1p_2\cdots p_n+1$ 不可能是

平方数.

81. 哪些正整数既不是合数又不是两个正的合数之和?

82. 若 p 和 q 为素数, 且 $p>q$, 证明: 若 $\phi(p^a)=\phi(q^b)$, 则 $a=1$. ($a>0$, 且 $b>0$.)

83.
$$2^2(2^3-1)=1^3+3^3;$$
$$2^4(2^5-1)=1^3+3^3+5^3+7^3;$$
$$2^6(2^7-1)=1^3+3^3+\cdots+15^3.$$
我们可能要推测, 除 6 以外的所有偶完全数都是由 1^3 开始的相继的奇数的立方和. 这对不对?

84. $1000\equiv1 \pmod{37}$. 据此提出一个整数可被 37 整除的判别方法.

85. (a) 求出所有构成算术级数的 x, y, z, 满足 $x^2+xy+y^2=z^2$, 且 $xy\neq0$;

(b) 求出所有构成算术级数的 x, y, z, 满足 $x^2+kxy+y^2=z^2$, 且 $xy\neq0$.

86. 若 a 和 b 为奇数, 证明下列方程有解:
$$x^2+y^2=(a^2+b^2)/2.$$

87. 若 n 是一个偶完全数, 证明: n 的各因子的调和平均数是一个整数.

88. 假定 $n^2+n+1=p^r$, 其中 $n\geqslant1$, p 为素数, $r\geqslant1$.

(a) 证明 p 为奇数;

(b) 证明: 若 $n\equiv1 \pmod 3$, 则唯一的解为 $n=1$, $p=3$, $r=1$;

(c) 证明 r 为奇数;

(d) 证明: 若 $p\neq3$, 则 $p\equiv1 \pmod 3$.

89. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$. 假定 a_n, a_0 和其余系数中的奇数个系数均为奇数, 证明 $f(x)=0$ 不存在有理

数根.

90. 若$n<p$, 且$(n, p-1)=1$, 证明$x^n\equiv n(\bmod p)$有解.

91. (a) 证明: 若$(a, p)=1$, $n|(p-1)$, 且$a^{(p-1)/n}\not\equiv 1(\bmod p)$, 则$a$不是一个$n$次剩余$(\bmod p)$;

(b) 2是一个五次剩余$(\bmod 31)$吗?

92. 证明: 若n是3的一个乘幂, 则$n|(2^n+1)$.

93. (a) 证明: 不可能成立$n^2+(n+1)^2=3m^2$;

(b) 对给定k, $k>0$,

$$n^2+(n+1)^2=km^2$$

有解的必要条件是什么?

94. 设m中不包含平方因子(即$m=p_1p_2\cdots p_k$是不同素数的乘积). 设想m有这样的性质: 若$p|m$, 则$(p-1)|m$.

(a) 说明$m=2, 6, 42$就具有上述性质;

(b) 还有其它m也具有上述性质吗?

(c) 还有多少这样的m呢?

95. 某人卖出n头牛, 每头牛价格为n元. 他用卖得的钱买了奇数只羊和一口猪, 每只羊的价格为10元, 一口猪的价格不到10元. 这口猪值多少钱?

96. 证明:

$$\prod_{n<p<2n} p \,\Big|\, \frac{(2n)!}{n!n!}.$$

97. 证明: 若p和$q=6p+1$为奇素数, 则3是q的一个原根.

98. 证明: 若$p=2^m+1$为素数, 则p的每个二次非剩余是p的一个原根.

99. 求$x(x-31)=y(y-41)$的正整数解.

100. 设c_0, c_1, c_2, c_3, c_4为任意整数, 又

$$f(x)=c_0+c_1\binom{x}{1}+2c_2\binom{x}{2}+6c_3\binom{x}{3}+12c_4\binom{x}{4}.$$

证明：给定 m，则对所有整数 n，有

$$m\mid(f(n+m)-f(n)).$$

$\left(\text{关于记号}\binom{x}{r}\text{，参见附录二.}\right)$

101．在 $\{6k+1\}(k=1,\ 2,\ \cdots)$ 这一序列中有着无限多个素数，下面是对这一命题的证明，补上未详细写出的部分：若 $p_1,\ p_2,\ \cdots,\ p_m$ 为所有形如 $6k+1$ 的素数，令 $N=p_1p_2\cdots p_m$，则 N^n+1 不能被 $p_1,\ p_2,\ \cdots,\ p_m$ 中任何一数整除．由于 $(N^3+1)/(N+1)$ 没有不是 $6k+1$ 这一形式的素因子，故必有一个因子大于 p_m．

102．证明：

$$\sum_{n=1}^{N}\sum_{d\mid n}f(d,\ n)=\sum_{m=1}^{N}\sum_{r=1}^{[N/m]}f(m,\ rm).$$

103．(a) 证明：若 r 和 s 满足 $5^ns-2^nr=1$ 和 $x=5^ns$，则 x^2 的最后 n 位数字与 x 的最后 n 位数字相同；

(b) 若 $n=3$，求出这样一个数 x．

104．确证下列判别素数的方法：若 α 是 1 的一个 n 次原根（即 $\alpha^n=1$，且对 $0<m<n$，有 $\alpha^m\neq1$），则

$$\frac{1}{n}\sum_{j=0}^{n-1}\alpha^{j(1+(n-1)!)}=\begin{cases}1, & \text{若 } n \text{ 为素数;}\\ 0, & \text{若 } n \text{ 为合数.}\end{cases}$$

105．证明：若 p 为任意奇素数，则序列 $\{2+np\}(n=1,\ 2,\ \cdots)$ 总包含有一个无穷的几何级数．

附录一　归纳法证明

在正文中，多次用到了数学归纳法这一证明方法. 本节的目的在于回忆一下这一方法的内容，并举例说明它是怎样使用的，还提供了一些习题作练习.

大家对数学有着一个不好的印象，总认为它是一门演绎推理的艺术：从一组假设出发，利用逻辑规则推出许多定理. 但这只是书本上给出的叙述方式，大多数新的数学内容却不是这样发现的. 要是有人一坐下来，就想："我现在要推理了"，用这种方式要证得任何有意义的事是不大可能的. 必须预见到一个目标，并猜想某个定理应当成立，然后根据你已有的知识将它推演出来，你觉得应该成立的那个定理总有个来源吧，而许多定理就是正确猜想的结果.

【练习 1】　根据下列数据猜出 $f(n)$：

n	0	1	2	3	4	5
$f(n)$	1	0	1	4	9	16.

【练习 2】　根据下列数据猜出 $f(n)$：

n	0	1	2	3	4	5	6
$f(n)$	1	2	5	10	17	26	37.

【练习 3】(选做)　根据下列数据猜想一个关于 $f(n)$ 的定理：

n	1	2	3	4	5	6	7
$f(n)$	2	-1	-2	-1	2	7	14.

由于数论研究的主要是正整数，因此有些定理的形式就

是："对所有正整数 n 某某事情成立."证明这类命题常常可用数学归纳法(或简称归纳法，别的归纳法我们就不讨论了)．这种证法是以正整数的下列性质为基础的：

(1)　　若整数的某一集合包含 1，且
　　　如它包含 r 就一定包含 $r+1$，
　　　则此集合包含了所有正整数.

(这是一个非常基本的性质，通常将它当作正整数的一个不加证明的公设来看待.)如我们要证关于正整数 n 的某个命题 $P(n)$ 对一切 n 成立($n=1, 2, \cdots$)，我们就要用到这一性质.下面是这类命题的几个例子：

$P_1(n)$："$n^2+3n+2>(n+1)^2-5$."

$P_2(n)$："$n(n+1)(n+2)$ 可被 6 整除."

$P_3(n)$："$f(x_1+x_2+\cdots+x_n) \geqslant f(x_1)+f(x_2)+\cdots+f(x_n)$."

设 S 表示使 $P(n)$ 成立的那些正整数的集合. 若我们能够证明，1 在 S 中，且若 r 在 S 中时 $r+1$ 也在 S 中，则(1)告诉我们，所有正整数都在 S 中. 换一种说法，我们就得归纳法原理：

若 $P(1)$ 成立，且
若 $P(r)$ 成立就能推得 $P(r+1)$ 也成立，
则 $P(n)$ 对所有 $n(n=1, 2, \cdots)$ 成立.

【练习 4】 填空：若 $P(17)$ 成立，且若 $P(r)$ 成立时 $P(r+1)$ 也成立，则对所有________，$P(n)$ 成立.

我们举一个大家熟悉的例子来说明用归纳法是怎么证明的. 设 $P(n)$ 是命题

$$“1+2+\cdots+n=n(n+1)/2.”$$

我们要用归纳法来证明：$P(n)$ 对所有正整数 n 成立.

【练习 5】 $P(1)$是什么？它成立吗？

假定 $P(r)$ 成立，也即假定

(2) $$1+2+\cdots+r=r(r+1)/2.$$

我们希望推得 $P(r+1)$成立，也就是要根据(2)证明

(3) $$1+2+\cdots+(r+1)=(r+1)(r+2)/2.$$

若在(2)之两端加上 $r+1$，我们得

$$\begin{aligned}1+2+\cdots+r+(r+1)&=r(r+1)/2+(r+1)\\&=(r+1)(r/2+1)=(r+1)(r+2)/2.\end{aligned}$$

它即为(3). 这样，归纳法原理的两部分都已证得，故 $P(n)$对所有正整数 n 成立.

用归纳法证题时，我们一定不可忘记证明 $P(1)$成立. 即使我们已经证得 $P(r)$成立时 $P(r+1)$也成立，但若 $P(1)$ 不成立，我们仍不能推断 $P(n)$对任何 n 都成立. 例如，设 $P(n)$为

$$n+(n+1)=2n.$$

假定 $P(r)$为真，也即假定

(4) $$r+(r+1)=2r,$$

利用它，我们可得

$$(r+1)+(r+2)=r+(r+1)+2=2r+2=2(r+1),$$

故 $P(r+1)$也真. 所以，要是 $P(1)$成立，就能推得 $P(n)$对所有正整数 n 成立. 由于 $P(1)$实际上并不成立，我们就不能下此结论. 事实上，$P(n)$对所有 n 都不成立.

用归纳法证明时，不用说，我们应该验证，$P(r)$为真时即能推得 $P(r+1)$也真. 例如，由下表

n	1	2	3	4	5	6
$f(n)$	2	4	6	8	10	12

我们还不能推断 $f(n)=2n$ 对一切 n 成立. 事实上，也可能有

$f(7)=\pi$, 因为在制表时我们心目中考虑的函数可能是

$$f(n)=2n+\frac{(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)(\pi-14)}{6\cdot5\cdot4\cdot3\cdot2}.$$

有时，我们也使用归纳法原理的另一种形式：

若 $P(1)$ 成立，且

若 $P(k)$ 对 $1\leqslant k\leqslant r$ 成立能推出 $P(r+1)$ 成立，

则 $P(n)$ 对所有 $n(n=1, 2, \cdots)$ 成立.

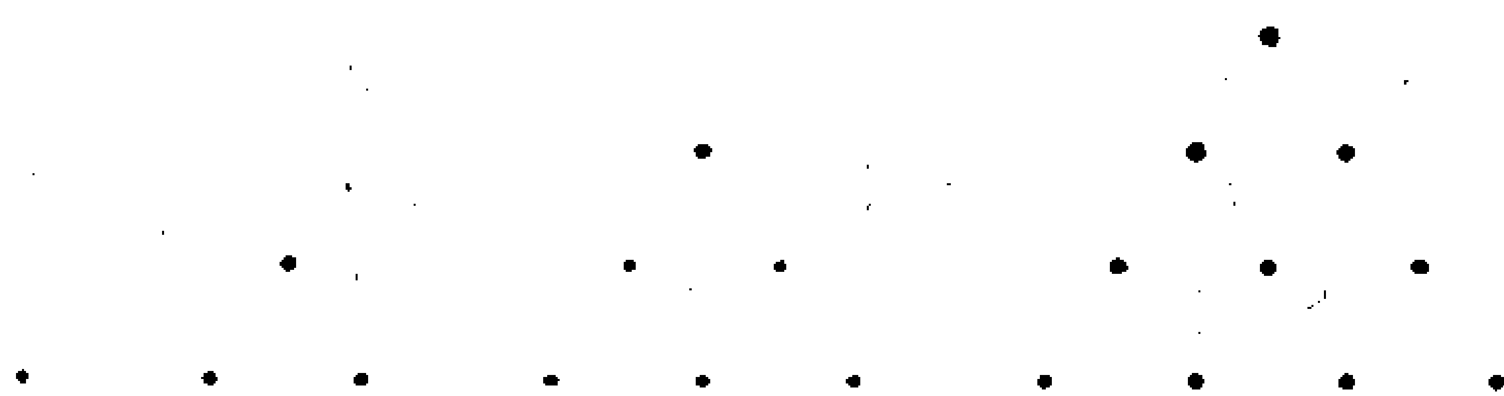
它之所以正确，是由于整数还有下列相应的性质：若整数的某一集合包含 1，且若它包含 1, 2, …, r, 它就也包含 $r+1$, 则它包含了所有的正整数.

习　题

1．证明：对 $n=2, 3, \cdots$, 成立，

$$1/1\cdot2+1/2\cdot3+\cdots+1/(n-1)n=1-(1/n).$$

2．1, 3, 6, 10 等叫做三角形数：



设 t_n 表示第 n 个三角形数，求 t_n 的公式.

3．证明：对 $n=1, 2, \cdots$, 有

$$1^2+2^2+\cdots+n^2=n(2n+1)(n+1)/6.$$

4．

$$1^3=1,$$
$$1^3+2^3=3^2,$$
$$1^3+2^3+3^3=6^2,$$
$$1^3+2^3+3^3+4^3=10^2.$$

猜想一个定理并证明之.

5．根据题 4 或者使用猜想和归纳法，对于 $k=1, 2, \cdots$, 为下列和式推

导一个公式:

$$1^3+3^3+5^3+\cdots+(2k-1)^3.$$

6. 假定 $a_1=1$, 且对 $n=1, 2, \cdots$, 有 $a_{n+1}=2a_n+1$, 用归纳法证明 $a_n=2^n-1$.

7. 假定 $a_0=a_1=1$, 且对 $n=1, 2, \cdots$, 有 $a_{n+1}=a_n+2a_{n-1}$, 用归纳法证明

$$a_n=\frac{2^{n+1}+(-1)^n}{3}.$$

8.
$$1\cdot2\cdot3\cdot4=5^2-1,$$
$$2\cdot3\cdot4\cdot5=11^2-1,$$
$$3\cdot4\cdot5\cdot6=19^2-1,$$
$$4\cdot5\cdot6\cdot7=29^2-1.$$

猜想一个定理并证明之.(也可不用归纳法证明.)

9. 对 $n=0, 1, \cdots$, 为下列和式猜想一个公式并证明之:

$$1^2+4^2+7^2+\cdots+(3n+1)^2.$$

10. 用归纳法证明:对 $n=1, 2, \cdots$, $n(n+1)(n+2)$ 可被 6 整除.

11. 作出函数 f 的一个公式,使

$$f(1)=f(2)=f(3)=f(4)=0,\quad f(5)=17.$$

12. 设 t_n 表示第 n 个三角形数,考虑下表:

n	1	2	3	4	5
t_n	1	3	6	10	15
$8t_n+1$	9	25	49	81	121.

最后一行全为平方数,这是一种偶然的巧合吗?

13. 用归纳法证明:对 $n=1, 2, \cdots$, n^5-n 可被 5 整除.

14. 斐波纳契(Fibonacci)数的定义由下式给出:

$$f_{n+1}=f_n+f_{n-1},\quad f_1=f_2=1.$$

证明:对 $n=1, 2, \cdots$, f_{5n} 可被 5 整除.

附录二　求和记号和其它记号

求和记号 Σ 的用处确实很大．通常使用这一记号时，求和变量应在标明的范围内取遍所有整数值：

$$\sum_{i=3}^{9} i^2=9+16+25+36+49+64+81;$$

$$\sum_{j=2}^{k} n/j=n/2+n/3+\cdots+n/k;$$

$$\sum_{k=1}^{n} kt_k=t_1+2t_2+3t_3+\cdots+nt_n;$$

$$\sum_{r=1}^{5} 1=1+1+1+1+1.$$

【练习 1】　详细写出：(a) $\sum_{r=1}^{6} f(r)g(7-r)$；(b) $\sum_{k=1}^{3}\varphi(k)/k$；(c) $\sum_{k=-1}^{1}\sum_{j=2}^{4} f(j)g(k)$．

【练习 2】　用求和记号写出：

(a) $1+2+3+\cdots+k$；

(b) $\frac{1}{3}+\frac{2}{5}+\frac{3}{7}+\cdots+\frac{17}{35}$；

(c) $2+\frac{3}{4}+\frac{4}{9}+\cdots+\frac{17}{256}$．

一般地，$\sum_{I} f(a)$ 告诉我们，应按规则 I 将 $f(a)$ 的各值相加，而规则 I 确定的是 a 值的一个集合．例如，

$$\sum_{d\mid n} f(d)$$

表示求和要对 n 的所有正因子进行：

$$\sum_{d|9} d^2 = 1^2+3^2+9^2;$$

$$\sum_{d|12}\sigma(d) = \sigma(1)+\sigma(2)+\sigma(3)+\sigma(4)+\sigma(6)+\sigma(12).$$

【练习 3】 计算：(a) $\sum_{d|6} 1/d$; (b) $\sum_{d|28} 1/3$; (c) $\sum_{d|15} 15/d$.

经常看到的另一种和式是

$$\sum_{p\leqslant x} f(p),$$

求和应对不大于 x 的所有素数进行．例如，

$$\sum_{p\leqslant 10} f(p) = f(2)+f(3)+f(5)+f(7).$$

因此，$\pi(x)$ 这一重要的函数（即小于或等于 x 的素数个数）可写为

$$\pi(x) = \sum_{p\leqslant x} 1.$$

事实上，我们可将所需要的任何形式的条件写在求和号下面或旁边．例如，

$$\sum_{\substack{(n,10)=1\\ n\leqslant 10}} n = 1+3+7+9;$$

$$\sum_{\substack{2\leqslant m\leqslant 6\\ 2\leqslant n\leqslant 6\\ (m,n)=1}} \frac{m}{n} = \frac{2}{3}+\frac{2}{5}+\frac{3}{2}+\frac{3}{4}+\frac{3}{5}+\frac{4}{3}$$

$$+\frac{4}{5}+\frac{5}{2}+\frac{5}{3}+\frac{5}{4}+\frac{5}{6}+\frac{6}{5};$$

$$\sum_{\substack{m+n=6\\ m,n\geqslant 1}} f(m,n) = f(1,5)+f(2,4)$$

$$+f(3,3)+f(4,2)+f(5,1).$$

【练习 4】 计算：

(a) $\sum_{p\leqslant 15} p$; (b) $\sum_{\substack{5|n\\ 0<n<49}} \frac{n}{5}$; (c) $\sum_{0<n^{1/2}\leqslant 99} 1$.

正如 Σ 代表和式，Π 代表积式，用其中一个记号可以做

到的事，用另一个记号也能做到．例如，

$$\prod_{k=1}^{n} k=n!;\quad \prod_{p\leq 7}\left(1-\frac{1}{p}\right)=\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7};$$

$$10\prod_{p\mid 10}\left(1-\frac{1}{p}\right)=10\cdot\frac{1}{2}\cdot\frac{4}{5};\quad \prod_{k=1}^{4}\frac{k+2}{k}=\frac{3}{1}\cdot\frac{4}{2}\cdot\frac{5}{3}\cdot\frac{6}{4}.$$

【练习 5】 计算：

$$\text{(a)}\ \prod_{k=1}^{17}1;\quad \text{(b)}\ \prod_{k=1}^{17}2;\quad \text{(c)}\ \prod_{p\leq 5}\frac{p}{p+2}.$$

最好要熟悉的另一个记号是最大整数记号：$[x]$表示不大于 x 的最大整数．（注意，本节中的 x 和 y 不一定表示整数，它们可取任意实数值，其它小写字母则仍代表整数．）换一种说法，此定义说明，$[x]$是满足

$$x-1<[x]\leq x$$

的唯一整数．再用另一种说法，就是：欲求$[x]$，可先在实数轴上找出 x，然后向左走，直到碰见一个整数为止，此整数即为$[x]$．还可用第四种说法：$[x]$是满足

$$[x]\leq x<[x]+1$$

的唯一整数．例如，$[2]=2$，$[5/2]=2$，$[\pi]=3$，$[-1/2]=-1$，$[-\pi]=-4$．

记号$[x]$有好几种读法："x 的整数部分"，这是一种很好的普通读法；"方括号 x"，这一读法也很普遍，但不大好．

【练习 6】 证明：$[x+1]=[x]+1$．你能将此推广吗？

【练习 7】 举出反例说明下列各式都不能对所有 x 和 y 成立：

$[x+y]=[x]+[y]$；$[x/y]=[x]/[y]$；$[xy]=[x][y]$．

作为应用最大整数记号的一例，我们证明

定理 1 在 b 的正倍数中，小于或等于 a 者个数为$[a/b]$．

证明 设所有小于或等于 a 的 b 的正倍数为

$$b,\ 2b,\ 3b,\ \cdots,\ kb.$$

由于它们皆小于或等于 a，我们有 $kb\leqslant a$，即 $k\leqslant a/b$. 另一方面，接在 kb 后面的 b 的下一个倍数大于 a:

$$(k+1)b>a, \quad 即 \quad k>a/b-1.$$

因此，b 的正倍数中小于或等于 a 者的个数 k 满足

$$a/b-1<k\leqslant a/b.$$

这是一个长度为 1 的区间，它只包含一个整数，就是 $[a/b]$. 因此 $k=[a/b]$，定理得证.

【练习 8】 在 1 与 1977 之间有多少个整数能被 11 整除?

与 $[x]$ 相联系的另一记号是小数部分记号. x 的小数部分记为 $\langle x\rangle$，它被定义为

$$\langle x\rangle=x-[x].$$

你可立即看出: $0\leqslant\langle x\rangle<1$; 而其它性质则留给读者去探讨.

本书正文中还用到了另外两个记号，对它们大家可能不大熟悉，我们也来提一提. 记号 $n!$ (读为"n 阶乘")是对正整数定义的，它表示从 1 到 n 的各个正整数的乘积，即对 $n=1, 2, \cdots$，有

$$n!=n(n-1)(n-2)\cdots3\cdot2\cdot1.$$

例如，$1!=1$, $4!=24$, $6!=720$. 另外，还规定 $0!=1$.

与阶乘记号有联系的是二项式系数(也称为组合记号)，记为 $\binom{n}{m}$. 对于 $n\geqslant m\geqslant0$，其定义是

$$\binom{n}{m}=\frac{n!}{m!(n-m!)}=\frac{n(n-1)\cdots(n-m+1)}{m(m-1)\cdots1}.$$

例如，

$$\binom{5}{3}=\frac{5!}{3!2!}=\frac{5\cdot4}{2\cdot1}=10;$$

$$\binom{10}{4}=\frac{10!}{4!6!}=\frac{10\cdot 9\cdot 8\cdot 7}{4\cdot 3\cdot 2\cdot 1}=210.$$

二项式系数的许多性质非常有用．例如，若 p 为素数，则对 $n=2, 3, \cdots, p-1$，有 $p\left|\binom{p}{n}\right.$．这种记号主要出现在二项式公式中：对任意实数 x 和 y（整数或非整数）以及任意正整数 n，有

$$(x+y)^n=\binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\cdots$$
$$+\binom{n}{n-1}xy^{n-1}+\binom{n}{n}y^n=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k.$$

习　题

1．计算：

(a) $\sum_{k=1}^{6}(k^2+k)$；　(b) $\sum_{k=1}^{\infty}1/2^k$；　(c) $\sum_{d|28}1/d$；

(d) $\sum_{\substack{k=1\\(k,3)=1}}^{9}k$；　(e) $\sum_{0<k<15}[k^{1/2}]$；　(f) $\sum_{p<50}p$.

2．用求和记号写出：

(a) $1+9+25+49+\cdots+169$；

(b) $\frac{1}{n}+\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}$；

(c) $a_0+a_1x+a_2x^2+\cdots+a_nx^n$；

(d) $u_rv_{n-r}+u_{r-1}v_{n-r+1}+\cdots+u_0v_n$.

3．证明或否定下列等式：

(a) $\sum_{k=1}^{n}(a_k+b_k)=\sum_{k=1}^{n}a_k+\sum_{k=1}^{n}b_k$；

(b) $\sum_{k=1}^{n}ca_k=c\sum_{k=1}^{n}a_k$；

(c) $\sum_{k=1}^{n}a_kb_k=\sum_{k=1}^{n}a_k\cdot\sum_{k=1}^{n}b_k$.

4. 计算:

(a) $(3^{1/2})^{[2^{1/2}]}$; (b) $[3^{1/2}]^{(2^{1/2})}$;

(c) $\prod_{k=1}^{6}[6/k]!$; (d) $\sum_{r=1}^{3}\sum_{k=1}^{r}k^r$;

(e) $\sum_{k=1}^{3}\sum_{r=1}^{k}k^r$.

5. 计算: (a) $8!$; (b) $\binom{8}{4}$; (c) $\binom{12}{5}$.

6. 证明: 对满足 $n\geqslant m>0$ 的整数 n 和 m, 有

$$\binom{n}{m}=\binom{n}{n-m}.$$

7. 用二项式公式展开:

(a) $(x+2)^6$; (b) $(1-a)^7$.

8. 用二项式公式化简:

(a) $x^3+9x^2+27x+27$;

(b) $\binom{n}{0}x^n-\binom{n}{1}x^{n-1}+\binom{n}{2}x^{n-2}-\cdots+(-1)^n\binom{n}{n}$.

9. 对 $k=1, 2, 3, 4$, 计算$[(3/2)^k]$.

10. 下列命题是否正确?

(a) 对一切实数 x, 有$[-x]=-[x]$;

(b) 对一切实数 x 和所有整数 n, 有$[n^x]=n^{[x]}$.

11. 令$\|x\|$表示最接近 x 的整数, 将$\|x\|$用最大整数记号表示出来.

12. $[x]+[-x]$可取哪些值?

13. 给定素数 p, 计算:

(a) $\sum_{\substack{k=1\\ p\nmid k}}^{p^2}1$; (b) $\sum_{\substack{k=1\\ p\nmid k}}^{n}1$.

14. 1902 和 2038 之间有多少个数是 7 的倍数?

15. 证明: 对所有整数 n 和函数 f, 有

$$\sum_{d|n}f(d)=\sum_{d|n}f(n/d).$$

16. 证明下列命题不成立: 对所有整数 n 和所有函数 f, 有

$$\sum_{p\leqslant n}f(p)=\sum_{p\leqslant n}f(n/p).$$

17. 证明:

$$\sum_{i=1}^{N}\sum_{j=1}^{N} f(i, j)=\sum_{j=1}^{N}\sum_{i=1}^{N} f(i, j).$$

18. 证明:

$$\sum_{i=1}^{N}\sum_{j=1}^{i} f(i, j)=\sum_{j=1}^{N}\sum_{i=j}^{N} f(i, j).$$

19. 证明:

$$\prod_{k=1}^{n} k^{[n/k]}=\prod_{k=1}^{n}[n/k]!.$$

20. 证明:对所有 $n>1$, 有

$$\frac{1}{n}\sum_{d\mid n} d>\frac{1}{n^2}\sum_{d\mid n} d^2.$$

21. 在区间 $x<n\leqslant y$ 中,共有多少个整数?

22. 证明:

$$\sum_{k=0}^{n-1}\langle k/n\rangle=\frac{n-1}{2}.$$

23. 假定 $\sum_{k=1}^{N} 1/n^k=1$, 且这些 n_k 都是正奇数,证明 N 也是奇数

附录三　模为合数的二次同余式

关于 $x^2 \equiv a \pmod p$ 我们已经知道得很多，但还没有学过模为合数的二次同余式：

(1)
$$Ax^2 + Bx + C \equiv 0 \pmod m.$$

本节中，我们要看一看(1)应如何求解.

我们首先考虑一种特殊情况：

(2)
$$x^2 \equiv a \pmod m.$$

与二次同余式 $(\bmod\ p)$ 不同，并非所有象(1)那样的同余式都能通过配方写成这一形式. 例如，$3x^2 + x + 1 \equiv 0 \pmod 9$ 就不能写成这种形式. 设 $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ 是 m 的素数幂分解式，则(2)之任一解都满足下列同余式组：

(3)
$$x^2 \equiv a \pmod{p_k^{e_k}}, \quad k = 1, 2, \cdots, n.$$

考虑到中国剩余定理，其逆也是正确的. 为了对任一 m 求解(2)，只要知道对所有素数 p 和正整数 e，如何求解

(4)
$$x^2 \equiv a \pmod{p^e}$$

就足够了. 例如，让我们来解 $x^2 \equiv 9 \pmod{28}$；我们将它分为几部分，对每部分求解，然后将它们重新并在一起. 我们首先解

(5)
$$x^2 \equiv 9 \pmod 4 \quad 和 \quad x^2 \equiv 9 \pmod 7.$$

第一个同余式的解为 1 和 3，第二个同余式的解为 3 和 4，因此(5)有四组解，它们是

(a)　$x \equiv 1 \pmod 4$　和　$x \equiv 3 \pmod 7$；

(b)　$x \equiv 1 \pmod 4$　和　$x \equiv 4 \pmod 7$；

(c) $x\equiv 3 \pmod 4$ 和 $x\equiv 3 \pmod 7$;

(d) $x\equiv 3 \pmod 4$ 和 $x\equiv 4 \pmod 7$.

所以，原来以 28 为模的同余式共有 4 个解，它们是：(a)17; (b)25; (c)3; (d)11.

若 $m=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$，且 $x^2\equiv a \pmod{p_k^{e_k}}$ 有 s_k 个解，则同余式组(3)有 $s_1s_2\cdots s_n$ 组不同的解，从而 $x^2\equiv a \pmod m$ 就有这一数目的解. 特别地，若(3)中任一同余式无解，则(2)也无解. 现在我们来看一看 $x^2\equiv a \pmod{p^e}$ 有多少解，然后再讨论如何将解求出来.

引理 1 若 p 为奇素数，$p\nmid a$，且 a 是一个二次剩余 $(\bmod p)$，则 $x^2\equiv a \pmod{p^e}$ 对每个正整数 e 恰有两解.

证明 我们用归纳法来证这一引理. 它对 $e=1$ 成立(参见 § 11). 假定它对 $e=k-1$ 成立，$k\geqslant 2$. 首先我们要证，$x^2\equiv a \pmod{p^{k-1}}$ 的每一解都可用来作出 $x^2\equiv a \pmod{p^k}$ 的两个解；然后我们将证明它们也是仅有的解. 设 r 为 $x^2\equiv a \pmod{p^{k-1}}$ 之一解，则对某 h，有

(6) $$r^2=a+hp^{k-1}.$$

考虑这样一些数：

$$R_j=r+jp^{k-1},\quad j=1,\ 2,\ \cdots.$$

我们有 $$R_j^2=r^2+2rjp^{k-1}+j^2p^{2k-2},$$

故 $$R_j^2\equiv a+hp^{k-1}+2rjp^{k-1}\equiv a+(h+2rj)p^{k-1} \pmod{p^k}.$$

若我们选取 j，使

$$R_j^2\equiv a \pmod{p^k},$$

即得 $x^2\equiv a \pmod{p^k}$ 的一解. 因此，要是有一个整数 j，使

$$h+2rj\equiv 0 \pmod p,$$

就能做到上面这一点. 由(6)知，这样的 j 是存在的，因为由 $(2r,\ p)=1$ 知，此同余式有唯一解. 我们举一个例子来说明

上述做法．从 $5^2\equiv7 \pmod 9$ 出发，作 $x^2\equiv7 \pmod{27}$ 的一解．令

$$R_j=5+9j,$$

所以，$$R_j^2=25+90j+81j^2\equiv25+9j \pmod{27}.$$

我们要找 j，使 $25+9j\equiv7 \pmod{27}$．$j=1$ 即能做到这一点．因此，14 就是 $x^2\equiv7 \pmod{27}$ 的一个解．

【练习 1】 验证：$14^2\equiv7 \pmod{27}$．

【练习 2】 求 $x^2\equiv7 \pmod{81}$ 的一个解．

我们已经证明 $x^2\equiv a \pmod{p^k}$ 有一解，将它叫做 s．则 p^k-s 为另一解．剩下来即要证明，不存在其它解．假定 t 是 $x^2\equiv a \pmod{p^k}$ 的任一解，我们要证，$t=s$ 或 $t=p^k-s$，这就可完成引理的证明．我们有 $t^2\equiv s^2 \pmod{p^k}$，故

$$p^k\mid(t-s)(t+s).$$

因为 $k\geqslant2$，只能有下列三种情况中的一种：

(i) $p^k\mid(t-s)$；

(ii) $p^k\mid(t+s)$；

(iii) $p\mid(t-s)$，且 $p\mid(t+s)$．

在第一种情况下，$t\equiv s \pmod{p^k}$，而因 t 和 s 都是最小剩余 $\pmod{p^k}$，故有 $t=s$；在第二种情况下，我们有 $t=p^k-s$；在第三种情况下，我们有 $p\mid2s$，因 p 是素数，故有 $p\mid s$．设 $s=ps_1$，由 $s^2\equiv a \pmod{p^k}$，可知对某 m，有

$$p^2s_1^2=a+mp^k,$$

因而 $a\equiv0 \pmod p$，这与 $p\nmid a$ 的假定矛盾．

【练习 3】 从 $2^2\equiv3^2\equiv44 \pmod 5$ 出发，找出 $x^2\equiv44 \pmod{125}$ 的所有解．

引理 1 只涉及奇素数，但还有 $p=2$ 的情况．这种情况稍微复杂些．若我们有 $x^2\equiv a \pmod{2^e}$，首先，我们可假定 a 为奇

数．（若不然，可用 2 的乘幂去除，直到求得一个 a 为奇数的同余式为止，例如，由 $x^2\equiv 12(\bmod 16)$，可得 $(x/2)^2\equiv 3(\bmod 4)$．）其次，还可假定 $a\equiv 1(\bmod 8)$，因为任何奇数的平方都与 1 同余 $(\bmod 8)$．下列引理完整地回答了求解 $x^2\equiv a(\bmod 2^e)$ 的问题．

引理 2 若 $a\equiv 1(\bmod 8)$，则按照 $e=1$，$e=2$ 或 $e\geqslant 3$，$x^2\equiv a(\bmod 2^e)$ 分别地恰有一个解，恰有两个解或恰有四个解．

证明 前两种情况是显然的．在第三种情况下，若 $e=3$，也很显然；故假定 $e\geqslant 4$．象我们在奇素数情况下所作的那样，要证 $x^2\equiv a(\bmod 2^e)$ 至少有四个解，可取对模 2^{e-1} 的一个解，再利用它去构造对模 2^e 的一个解．假定 $r^2\equiv a(\bmod 2^{e-1})$，则对某 h，有 $r^2=a+h2^{e-1}$．令 $R_j=r+j2^{e-2}$，则

$$R_j^2=r^2+2rj2^{e-2}+j^22^{2e-4}\equiv a+(h+rj)2^{e-1}(\bmod 2^e).$$

所以，要有 $R_j^2\equiv a(\bmod 2^e)$，只需取 j，使 $h+rj\equiv 0(\bmod 2)$．由于 r 为奇数，这总是能办到的．因此，$x^2\equiv a(\bmod 2^{e-1})$ 的任一解都能产生出 $x^2\equiv a(\bmod 2^e)$ 的一个解来．

例如，我们来求 $x^2\equiv 17(\bmod 64)$ 的一个解．由 $1^2\equiv 17(\bmod 16)$ 出发，令 $R_j=1+8j$，则

$$R_j^2=1^2+16j+64j^2\equiv 1+16j(\bmod 32).$$

若要它变成 $17(\bmod 32)$．可取 $j=1$，因此，$9^2\equiv 17(\bmod 32)$．为了使幂次再增加 1，可令 $S_j=9+16j$，则

$$S_j^2=81+18\cdot 16j+256j^2\equiv 17+18\cdot 16j(\bmod 64).$$

取 $j=0$，即得 $9^2\equiv 17(\bmod 64)$．

【练习 4】 求 $x^2\equiv 17(\bmod 128)$ 的一个解．

【练习 5】 若 r 满足 $x^2\equiv a(\bmod 2^e)$，证明 2^e-r，$2^{e-1}-r$，$2^{e-1}+r$ 也都满足此同余式．

【练习 6】 由 $9^2\equiv 17(\bmod 64)$，求出其它三个解．

余下来要证，对于 $a\equiv 1 \pmod 8$ 和 $e\geqslant 3$，$x^2\equiv a \pmod{2^e}$ 不可能多于四个解. 利用归纳法、练习 5 及证明引理 1 时所用的想法即可证得这一点. 由于想法是一样的，我们就不详细论证了.

借助于引理 1 和引理 2，我们一看到形为 $x^2\equiv a \pmod m$ 的一个同余式，几乎马上就可说出它有多少解. 例如，$x^2\equiv 9 \pmod{1200}$ 有 8 个解，这是因为，$1200=2^4\cdot 3\cdot 5^2$，而 $x^2\equiv 9 \pmod{2^4}$ 有 4 个解，$x^2\equiv 9 \pmod 3$ 有 1 个解，$x^2\equiv 9 \pmod{25}$ 有 2 个解.

【练习 7】 $x^2\equiv 10 \pmod{1200}$ 有多少解?

求解一般同余式 $Ax^2+Bx+C\equiv 0 \pmod m$ 和求解 $x^2\equiv a \pmod m$ 的方法相同: 将它分成几部分，

$$Ax^2+Bx+C\equiv 0 \pmod{p^e},$$

从 $Ax^2+Bx+C\equiv 0 \pmod p$ 开始，先求出其解（根据§11 我们知道如何求解），利用它的解逐步求出对模 p^2，p^3，…，p^e 的解. 然后将各部分的解并在一起而得对模 m 的解. 在一般情况下，要说出 $Ax^2+Bx+C\equiv 0 \pmod m$ 具有多少个解是困难的，因为由解 $\pmod{p^{k-1}}$ 过渡到解 $\pmod{p^k}$ 时，从一个解求得的新解可能有 p 个，也可能只有一个或一个也没有，这就取决于此二次式的形式了. 不过，$Ax^2+Bx+C\equiv 0 \pmod{p^e}$ 的全部解总能用上述方法求出. 这一点我们就不证明了，仅举两例来说明会发生什么样的情况. 让我们试一试来解

$$x^2+x+1\equiv 0 \pmod{27}. \tag{7}$$

我们知 $1^2+1+1\equiv 0 \pmod 3$，故欲求对模 9 的解，可设 $R_j=1+3j$. 那么，

$$\begin{aligned}R_j^2+R_j+1&=(1+6j+9j^2)+(1+3j)+1\\&=3+9j+9j^2\equiv 3 \pmod 9.\end{aligned}$$

于是，没有一个 j 的值能使 $R_j^2+R_j+1$ 与零同余(mod 9)．所以，(7)无解．

一个根也可以产生出 p 个根来，现举一例：

(8) $$x^2+x+7\equiv 0 \pmod{27}.$$

只有 $x\equiv 1 \pmod 3$ 才能满足 $x^2+x+7\equiv 0 \pmod 3$．若 $R_j=1+3j$，则

$$R_j^2+R_j+1=9+9j+9j^2,$$

对所有 j 的值，它都与零同余(mod 9)．因此，$x\equiv 1$, 4 或 7 都满足

$$x^2+x+7\equiv 0 \pmod 9.$$

现在我们必须让每一个根再增加一次幂而求得 (8) 的解．如设 $S_j=1+9j$，则

$$S_j^2+S_j+7=(1+18j+81j^2)+(1+9j)+7\equiv 9 \pmod{27},$$

任何 j 值都不会使左端为零(mod 27)，因而对模 9 的根 1 产生不出对模 27 的根来．下一步取 4 这个根：若 $T_j=4+9j$，则

$$T_j^2+T_j+7=(16+72j+81j^2)+(4+9j)+7$$
$$\equiv 27+81j\equiv 0 \pmod{27}.$$

因此，对所有 j，都有 $T_j^2+T_j+7\equiv 0 \pmod{27}$，它给出了(8)的三个根，即 4, 13, 22．

【练习 8】 说明对模 9 的根 7 产生不出对模 27 的根来．

于是，(8)恰有三解：$x=4$, $x=13$, $x=22$．

习　题

1．解下列同余式：

(a) $x^2\equiv 7 \pmod{243}$； (b) $x^2\equiv 44 \pmod{625}$；

(c) $x^2\equiv 17 \pmod{256}$．

2．求解 $x^2+x+7\equiv 0 \pmod{81}$．

3. 下列同余式各有多少解?

   (a) $x^2 \equiv 189 \pmod{900}$; (b) $x^2 \equiv 89 \pmod{1000}$;

   (c) $x^2 \equiv -11 \pmod{1100}$.

4. 对题3中每一同余式,至少求出三个解.

5. $3x^2+2x+1 \equiv 134 \pmod{800}$有多少解?

6. 证明: 任一 $x \equiv 33 \pmod{40}$ 满足上题中之同余式.

7. $x^2 \equiv a \pmod{400}$可能会有多少个解? 对每一种解的数目的情况各举一例说明之.

8. 证明: 若对 $e \geqslant 2$, r 是 $x^3 \equiv a \pmod{3^e}$的一解,则 $3^{e-1}+r$ 也满足此同余式. $3^{e-1}-r$ 和 3^e-r 是否满足此同余式?

9. 求解: (a) $x^3 \equiv 5 \pmod{16}$; (b) $x^3 \equiv 10 \pmod{27}$.

附 录 四

表 A 10,000 以内的整数的最小素因子表

下表给出了每个正奇数 n($3\leqslant n\leqslant 9999$, 且 n 不能被 5 整除)的最小素因子. 每列顶上各数(1, 3, 7, 9) 指出 n 的个位数, 而下面左边的数字指出 n 的千位数、百位数和十位数. 表中短划"-"说明 n 是素数.

例如, 在表中查到 102 那行时, 我们发现 1021 是素数, 1023 可被 3 整除, 1027 可被 13 整除, 1029 可被 3 整除. 借助此表可以迅速地求出 10,000 以内的任一整数 (及 20,000 以内的任一偶数)的素数幂分解式. 例如, 取 3141: 由表的 314 所在行, 我们发现 $3\mid 3141$, 相除可得 $3141=3\cdot 1047$; 由表的 104 所在行, 知 $3\mid 1047$, 故 $3141=3^2\cdot 349$; 而 34 所在行表明, 349 是素数, 故我们已求出 3141 的素数幂分解式.

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
0		—	—	3	10	—	—	—	—	20	3	7	3	11	30	7	3	—	3
1	—	—	—	—	11	3	—	3	7	21	—	3	7	3	31	—	—	—	11
2	3	—	3	—	12	11	3	—	3	22	13	—	—		32	3	17	3	7
3	—	3	—	3	13	—	7	—	—	23	3	—	3		33	—	3	—	3
4	—	—	—	7	14	3	11	3	—	24	—	3	13	3	34	11	7	—	—
5	3	—	3	—	15	—	3	—	3	25	—	11	—	7	35	3	—	3	—
6	—	3	—	3	16	7	—	—	13	26	3	—	3	—	36	19	3	—	3
7	—	—	7	—	17	3	—	3	—	27	—	3	—	3	37	7	—	13	—
8	3	—	3	—	18	—	3	11	3	28	—	—	7	17	38	3	—	3	—
9	7	3	—	3	19	—	—	—	—	29	3	—	3	13	39	17	3	—	3

表 A （续）

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
40	—	13	11	—	70	—	19	7	—	100	7	17	19	—	130	—	—	—	7
41	3	7	3	—	71	3	23	3	—	101	3	—	3	—	131	3	13	3	—
42	—	3	7	3	72	7	3	—	3	102	—	3	13	3	132	—	3	—	3
43	—	—	19	—	73	17	—	11	—	103	—	—	17	—	133	11	31	7	13
44	3	—	3	—	74	3	—	3	7	104	3	7	3	—	134	3	17	3	19
45	11	3	—	3	75	—	3	—	3	105	—	3	7	3	135	7	3	23	3
46	—	—	—	7	76	—	7	13	—	106	—	—	11	—	136	—	29	—	37
47	3	11	3	—	77	3	—	3	19	107	3	29	3	13	137	3	—	3	7
48	13	3	—	3	78	11	3	—	3	108	23	3	—	3	138	—	3	19	3
49	—	17	7	—	79	7	13	—	17	109	—	—	—	7	139	13	7	11	—
50	3	—	3	—	80	3	11	3	—	110	3	—	3	—	140	3	23	3	—
51	7	3	11	3	81	—	3	19	3	111	11	3	—	3	141	17	3	13	3
52	—	—	17	23	82	—	—	—	—	112	19	—	7	—	142	7	—	—	—
53	3	13	3	7	83	3	7	3	—	113	3	11	3	17	143	3	—	3	—
54	—	3	—	3	84	29	3	7	3	114	7	3	31	3	144	11	3	—	3
55	19	7	—	13	85	23	—	—	—	115	—	—	13	19	145	—	—	31	—
56	3	—	3	—	86	3	—	3	11	116	3	—	3	7	146	3	7	3	13
57	—	3	—	3	87	13	3	—	3	117	—	3	11	3	147	—	3	7	3
58	7	11	—	19	88	—	—	—	7	118	—	7	—	29	148	—	—	—	—
59	3	—	3	—	89	3	19	3	29	119	3	—	3	11	149	3	—	3	—
60	—	3	—	3	90	17	3	—	3	120	—	3	17	3	150	19	3	11	3
61	13	—	—	—	91	—	11	7	—	121	7	—	—	23	151	—	17	37	7
62	3	7	3	17	92	3	13	3	—	122	3	—	3	—	152	3	—	3	11
63	—	3	7	3	93	7	3	—	3	123	—	3	—	3	153	—	3	29	3
64	—	—	—	11	94	—	23	—	13	124	17	11	29	—	154	23	—	7	—
65	3	—	3	—	95	3	—	3	7	125	3	7	3	—	155	3	—	3	—
66	—	3	23	3	96	31	3	—	3	126	13	3	7	3	156	7	3	—	3
67	11	—	—	7	97	—	7	—	11	127	31	19	—	—	157	—	11	19	—
68	3	—	3	13	98	3	—	3	23	128	3	—	3	—	158	3	—	3	7
69	—	3	17	3	99	—	3	—	3	129	—	3	—	3	159	37	3	—	3

表 A　　　　(续)

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
160	—	7	—	—	190	—	11	—	23	220	31	—	—	47	250	41	—	23	13
161	3	—	3	—	191	3	—	3	19	221	3	—	3	7	251	3	7	3	11
162	—	3	—	3	192	17	3	41	3	222	—	3	17	3	252	—	3	7	3
163	7	23	—	11	193	—	—	13	7	223	23	7	—	—	253	—	17	43	—
164	3	31	3	17	194	3	29	3	—	224	3	—	3	13	254	3	—	3	—
165	13	3	—	3	195	—	3	19	3	225	—	3	37	3	255	—	3	—	3
166	11	—	—	—	196	37	13	7	11	226	7	31	—	—	256	13	11	17	7
167	3	7	3	23	197	3	—	3	—	227	3	—	3	43	257	3	31	3	—
168	41	3	7	3	198	7	3	—	3	228	—	3	—	3	258	29	3	13	3
169	19	—	—	—	199	11	—	—	—	229	29	—	—	11	259	—	—	7	23
170	3	13	3	—	200	3	—	3	7	230	3	7	3	—	260	3	19	3	—
171	29	3	17	3	201	—	3	—	3	231	—	3	7	3	261	7	3	—	3
172	—	—	11	7	202	43	7	—	—	232	11	23	13	17	262	—	43	37	11
173	3	—	3	37	203	3	19	3	—	233	3	—	3	—	263	3	—	3	7
174	—	3	—	3	204	13	3	23	3	234	—	3	—	3	264	19	3	—	3
175	17	—	7	—	205	7	—	11	29	235	—	13	—	7	265	11	7	—	—
176	3	41	3	29	206	3	—	3	—	236	3	17	3	23	266	3	—	3	17
177	7	3	—	3	207	19	3	31	3	237	—	3	—	3	267	—	3	—	3
178	13	—	—	—	208	—	—	—	—	238	—	—	7	—	268	7	—	—	—
179	3	11	3	7	209	3	7	3	—	239	3	—	3	—	269	3	—	3	—
180	—	3	13	3	210	11	3	7	3	240	7	3	29	3	270	37	3	—	3
181	—	7	23	17	211	—	—	29	13	241	—	19	—	41	271	—	—	11	—
182	3	—	3	31	212	3	11	3	—	242	3	—	3	7	272	3	7	3	—
183	—	3	11	3	213	—	3	—	3	243	11	3	—	3	273	—	3	7	3
184	7	19	—	43	214	—	—	19	7	244	—	7	—	31	274	—	13	41	—
185	3	17	3	11	215	3	—	3	17	245	3	11	3	—	275	3	—	3	31
186	—	3	—	3	216	—	3	11	3	246	23	3	—	3	276	11	3	—	3
187	—	—	—	—	217	13	41	7	—	247	7	—	—	37	277	17	47	—	7
188	3	7	3	—	218	3	37	3	11	248	3	13	3	19	278	3	11	3	—
189	31	3	7	3	219	7	3	13	3	249	47	3	11	3	279	—	3	—	3

表 A (续)

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
280	—	—	7	53	310	7	29	13	—	340	19	41	—	7	370	—	7	11	—
281	3	29	3	—	311	3	11	3	—	341	3	—	3	13	371	3	47	3	—
282	7	3	11	3	312	—	3	53	3	342	11	3	23	3	372	61	3	—	3
283	19	—	—	17	313	31	13	—	43	343	47	—	7	19	373	7	—	37	—
284	3	—	3	7	314	3	7	3	47	344	3	11	3	—	374	3	19	3	23
285	—	3	—	3	315	23	3	7	3	345	7	3	—	3	375	11	3	13	3
286	—	7	47	19	316	29	—	—	—	346	—	—	—	—	376	—	53	—	—
287	3	13	3	—	317	3	19	3	11	347	3	23	3	7	377	3	7	3	—
288	43	3	—	3	318	—	3	—	3	348	59	3	11	3	378	19	3	7	3
289	7	11	—	13	319	—	31	23	7	349	—	7	13	—	379	17	—	—	29
290	3	—	3	—	320	3	—	3	—	350	3	31	3	11	380	3	—	3	13
291	41	3	—	3	321	13	3	—	3	351	—	3	—	3	381	37	3	11	3
292	23	37	—	29	322	—	11	7	—	352	7	13	—	—	382	—	—	43	7
293	3	7	3	—	323	3	53	3	41	353	3	—	3	—	383	3	—	3	11
294	17	3	7	3	324	7	3	17	3	354	—	3	—	3	384	23	3	—	3
295	13	—	—	11	325	—	—	—	—	355	53	11	—	—	385	—	—	7	17
296	3	—	3	—	326	3	13	3	7	356	3	7	3	43	386	3	—	3	53
297	—	3	13	3	327	—	3	29	3	357	—	3	7	3	387	7	3	—	3
298	11	19	29	7	328	17	7	19	11	358	—	—	17	37	388	—	11	13	—
299	3	41	3	—	329	3	37	3	—	359	3	—	3	59	389	3	17	3	7
300	—	3	31	3	330	—	3	—	3	360	13	3	—	3	390	47	3	—	3
301	—	23	7	—	331	7	—	31	—	361	23	—	—	7	391	—	7	—	—
302	3	—	3	13	332	3	—	3	—	362	3	—	3	19	392	3	—	3	—
303	7	3	—	3	333	—	3	47	3	363	—	3	—	3	393	—	3	31	3
304	—	17	11	—	334	13	—	—	17	364	11	—	7	41	394	7	—	—	11
305	3	43	3	7	335	3	7	3	—	365	3	13	3	—	395	3	59	3	37
306	—	3	—	3	336	—	3	7	3	366	7	3	19	3	396	17	3	—	3
307	37	7	17	—	337	—	—	11	31	367	—	—	—	13	397	11	29	41	23
308	3	—	3	—	338	3	17	3	—	368	3	29	3	7	398	3	7	3	—
309	11	3	19	3	339	—	3	43	3	369	—	3	—	3	399	13	3	7	3

表 A (续)

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
400	—	—	—	19	430	11	13	59	31	460	43	—	17	11	490	13	—	7	—
401	3	—	3	—	431	3	19	3	7	461	3	7	3	31	491	3	17	3	—
402	—	3	—	3	432	29	3	—	3	462	—	3	7	3	492	7	3	13	3
403	29	37	11	7	433	61	7	—	—	463	11	41	—	—	493	—	—	—	11
404	3	13	3	—	434	3	43	3	—	464	3	—	3	—	494	3	—	3	7
405	—	3	—	3	435	19	3	—	3	465	—	3	—	3	495	—	3	—	3
406	31	17	7	13	436	7	—	11	17	466	59	—	13	7	496	11	7	—	—
407	3	—	3	—	437	3	—	3	29	467	3	—	3	—	497	3	—	3	13
408	7	3	61	3	438	13	3	41	3	468	31	3	43	3	498	17	3	—	3
409	—	—	17	—	439	—	23	—	53	469	—	13	7	37	499	7	—	19	—
410	3	11	3	7	440	3	7	3	—	470	3	—	3	17	500	3	—	3	—
411	—	3	23	3	441	11	3	7	3	471	7	3	53	3	501	—	3	29	3
412	13	7	—	—	442	—	—	19	43	472	—	—	29	—	502	—	—	11	47
413	3	—	3	—	443	3	11	3	23	473	3	—	3	7	503	3	7	3	—
414	41	3	11	3	444	—	3	—	3	474	11	3	47	3	504	71	3	7	3
415	7	—	—	—	445	—	61	—	7	475	—	7	67	—	505	—	31	13	—
416	3	23	3	11	446	3	—	3	41	476	3	11	3	19	506	3	61	3	37
417	43	3	—	3	447	17	3	11	3	477	13	3	17	3	507	11	3	—	3
418	37	47	53	59	448	—	—	7	67	478	7	—	—	—	508	—	13	—	7
419	3	7	3	13	449	3	—	3	11	479	3	—	3	—	509	3	11	3	—
420	—	3	7	3	450	7	3	—	3	480	—	3	11	3	510	—	3	—	3
421	—	11	—	—	451	13	—	—	—	481	17	—	—	61	511	19	—	7	—
422	3	41	3	—	452	3	—	3	7	482	3	7	3	11	512	3	47	3	23
423	—	3	19	3	453	23	3	13	3	483	—	3	7	3	513	7	3	11	3
424	—	—	31	7	454	19	7	—	—	484	47	29	37	13	514	53	37	—	19
425	3	—	3	—	455	3	29	3	47	485	3	23	3	43	515	3	—	3	7
426	—	3	17	3	456	—	3	—	3	486	—	3	31	3	516	13	3	—	3
427	—	—	7	11	457	7	17	23	19	487	—	11	—	7	517	—	7	31	—
428	3	—	3	—	458	3	—	3	13	488	3	19	3	—	518	3	71	3	—
429	7	3	—	3	459	—	3	—	3	489	67	3	59	3	519	29	3	—	3

表 A)　　　　　　　　　　　　　　　　　　　　　　　　　　(续)

	1 3 7 9		1 3 7 9		1 3 7 9		1 3 7 9
520	71141—	550	——— 7	580	— 7—37	610	—173141
521	313 317	551	337 3—	581	3— 311	611	3— 329
522	23 3— 3	552	— 3— 3	582	— 3— 3	612	— 311 3
523	———13	553	—11 729	583	71913—	613	——17 7
524	3 7 329	554	323 331	584	3— 3—	614	3— 311
525	59 3 7 3	555	7 3— 3	585	— 3— 3	615	— 347 3
526	—192311	556	67—19—	586	—11——	616	61— 731
527	3— 3—	557	3— 3 7	587	3 7 3—	617	3— 337
528	— 317 3	558	— 337 3	588	— 3 7 3	618	7 323 3
529	1167— 7	559	— 72911	589	4371—17	619	4111——
530	3— 3—	560	313 371	590	3— 319	620	3— 3 7
531	47 313 3	561	31 341 3	591	23 361 3	621	— 3— 3
532	17— 773	562	7—1713	592	31—— 7	622	— 713—
533	3— 319	563	343 3—	593	317 3—	623	323 317
534	7 3— 3	564	— 3— 3	594	13 319 3	624	79 3— 3
535	—531123	565	—————	595	11— 759	625	713—11
536	331 3 7	566	3 7 3—	596	367 347	626	3— 3—
537	41 319 3	567	53 3 7 3	597	7 343 3	627	— 3— 3
538	— 7—17	568	13—11—	598	—31—53	628	1161—19
539	3— 3—	569	3— 341	599	313 3 7	629	3 7 3—
540	11 3— 3	570	— 313 3	600	17 3— 3	630	— 3 7 3
541	7———	571	—29— 7	601	— 71113	631	—59—71
542	311 361	572	359 317	602	319 3—	632	3— 3—
543	— 3— 3	573	11 3— 3	603	37 3— 3	633	13 3— 3
544	——13—	574	—— 7—	604	7——23	634	17—11 7
545	3 7 353	575	311 313	605	3— 373	635	3— 3—
546	43 3 7 3	576	7 373 3	606	11 3— 3	636	— 3— 3
547	—13——	577	292353—	607	13—59—	637	23— 7—
548	3— 311	578	3— 3 7	608	3 7 3—	638	313 3—
549	17 323 3	579	— 311 3	609	— 3 7 3	639	7 3— 3

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
640	37	19	43	13	670	—	—	19	—	700	—	47	7	43	730	7	67	—	—
641	3	11	3	7	671	3	7	3	—	701	3	—	3	—	731	3	71	3	13
642	—	3	—	3	672	11	3	7	3	702	7	3	—	3	732	—	3	17	3
643	59	7	41	47	673	53	—	—	23	703	79	13	31	—	733	—	—	11	41
644	3	17	3	—	674	3	11	3	17	704	3	—	3	7	734	3	7	3	—
645	—	3	11	3	675	43	3	29	3	705	11	3	—	3	735	—	3	7	3
646	7	23	29	—	676	—	—	67	7	706	23	7	37	—	736	17	37	53	—
647	3	—	3	11	677	3	13	3	—	707	3	11	3	—	737	3	73	3	47
648	—	3	13	3	678	—	3	11	3	708	73	3	19	3	738	11	3	83	3
649	—	43	73	67	679	—	—	7	13	709	7	41	47	31	739	19	—	13	7
650	3	7	3	23	680	3	—	3	11	710	3	—	3	—	740	3	11	3	31
651	17	3	7	3	681	7	3	17	3	711	13	3	11	3	741	—	3	—	3
652	—	11	61	—	682	19	—	—	—	712	—	17	—	—	742	41	13	7	17
653	3	47	3	13	683	3	—	3	7	713	3	7	3	11	743	3	—	3	43
654	31	3	—	3	684	—	3	41	3	714	37	3	7	3	744	7	3	11	3
655	—	—	79	7	685	13	7	—	19	715	—	23	17	—	745	—	29	—	—
656	3	—	3	—	686	3	—	3	—	716	3	13	3	67	746	3	17	3	7
657	—	3	—	3	687	—	3	13	3	717	71	3	—	3	747	31	3	—	3
658	—	29	7	11	688	7	—	71	83	718	43	11	—	7	748	—	7	—	—
659	3	19	3	—	689	3	61	3	—	719	3	—	3	23	749	3	59	3	—
660	7	3	—	3	690	67	3	—	3	720	19	3	—	3	750	13	3	—	3
661	11	17	13	—	691	—	31	—	11	721	—	—	7	—	751	7	11	—	73
662	3	37	3	7	692	3	7	3	13	722	3	31	3	—	752	3	—	3	—
663	19	3	—	3	693	29	3	7	3	723	7	3	—	3	753	17	3	—	3
664	29	7	17	61	694	11	53	—	—	724	13	—	—	11	754	—	19	—	—
665	3	—	3	—	695	3	17	3	—	725	3	—	3	7	755	3	7	3	—
666	—	3	59	3	696	—	3	—	3	726	53	3	13	3	756	—	3	7	3
667	7	—	11	—	697	—	19	—	7	727	11	7	19	29	757	67	—	—	11
668	3	41	3	—	698	3	—	3	29	728	3	—	3	37	758	3	—	3	—
669	—	3	37	3	699	—	3	—	3	729	23	3	—	3	759	—	3	71	3

表 *A* (续)

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
760	11	—	—	7	790	—	7	—	11	820	59	13	29	—	850	—	11	47	67
761	3	23	3	19	791	3	41	3	—	821	3	43	3	—	851	3	—	3	7
762	—	3	29	3	792	89	3	—	3	822	—	3	19	3	852	—	3	—	3
763	13	17	7	—	793	7	—	—	17	823	—	—	—	7	853	19	7	—	—
764	3	—	3	—	794	3	13	3	—	824	3	—	3	73	854	3	—	3	83
765	7	3	13	3	795	—	3	73	3	825	37	3	23	3	855	17	3	43	3
766	47	79	11	—	796	19	—	31	13	826	11	—	7	—	856	7	—	13	11
767	3	—	3	7	797	3	7	3	79	827	3	—	3	17	857	3	—	3	23
768	—	3	—	3	798	23	3	7	3	828	7	3	—	3	858	—	3	31	3
769	—	7	43	—	799	61	—	11	19	829	—	—	—	43	859	11	13	—	—
770	3	—	3	13	800	3	53	3	—	830	3	19	3	7	860	3	7	3	—
771	11	3	—	3	801	—	3	—	3	831	—	3	—	3	861	79	3	7	3
772	7	—	—	59	802	13	71	23	7	832	53	7	11	—	862	37	—	—	—
773	3	11	3	71	803	3	29	3	—	833	3	13	3	31	863	3	89	3	53
774	—	3	61	3	804	11	3	13	3	834	19	3	17	3	864	—	3	—	3
775	23	—	—	—	805	83	—	7	—	835	7	—	61	13	865	41	17	11	7
776	3	7	3	17	806	3	11	3	—	836	3	—	3	—	866	3	—	3	—
777	19	3	7	3	807	7	3	41	3	837	11	3	—	3	867	13	3	—	3
778	31	43	13	—	808	—	59	—	—	838	17	83	—	—	868	—	19	7	—
779	3	—	3	11	809	3	—	3	7	839	3	7	3	37	869	3	—	3	—
780	29	3	37	3	810	—	3	11	3	840	31	3	7	3	870	7	3	—	3
781	73	13	—	7	811	—	7	—	23	841	13	47	19	—	871	31	—	23	—
782	3	—	3	—	812	3	—	3	11	842	3	—	3	—	872	3	11	3	7
783	41	3	17	3	813	47	3	79	3	843	—	3	11	3	873	—	3	—	3
784	—	11	7	47	814	7	17	—	29	844	23	—	—	7	874	—	7	—	13
785	3	—	3	29	815	3	31	3	41	845	3	79	3	11	875	3	—	3	19
786	7	3	—	3	816	—	3	—	3	846	—	3	—	3	876	—	3	11	3
787	17	—	—	—	817	—	11	13	—	847	43	37	7	61	877	7	31	67	—
788	3	—	3	7	818	3	7	3	19	848	3	17	3	13	878	3	—	3	11
789	13	3	53	3	819	—	3	7	3	849	7	3	29	3	879	59	3	19	3

	1 3 7 9		1 3 7 9		1 3 7 9		1 3 7 9
880	13 — — 23	910	19 — 7 —	940	7 — 23 97	970	89 31 17 7
881	3 7 3 —	911	313 311	941	3 — 3 —	971	311 3 —
882	— 3 7 3	912	7 3 — 3	942	— 311 3	972	— 371 3
883	— 11 — —	913	23 — — 13	943	— — — —	973	37 — 7 —
884	337 3 —	914	341 3 7	944	3 7 311	974	3 — 3 —
885	53 317 3	915	— 3 — 3	945	13 3 7 3	975	7 311 3
886	— — — 7	916	— 7 89 53	946	— — — 17	976	43 13 — —
887	319 313	917	3 — 367	947	3 — 3 —	977	329 3 7
888	83 3 — 3	918	— 3 — 3	948	19 353 3	978	— 3 — 3
889	17 — 7 11	919	7 29 17 —	949	— 11 — 7	979	— 7 97 41
890	329 359	920	3 — 3 —	950	313 337	980	3 — 317
891	7 337 3	921	61 313 3	951	— 331 3	981	— 3 — 3
892	11 — 79 —	922	— 23 — 11	952	— 89 713	982	7 11 31 —
893	3 — 3 7	923	3 7 3 —	953	3 — 3 —	983	3 — 3 —
894	— 323 3	924	— 3 7 3	954	7 3 — 3	984	13 343 3
895	— 7 13 17	925	11 19 — 47	955	— 41 19 11	985	— 59 — —
896	3 — 3 —	926	359 313	956	373 3 7	986	3 7 371
897	— 347 3	927	73 3 — 3	957	17 361 3	987	— 3 7 3
898	7 13 11 89	928	— — 37 7	958	11 7 — 43	988	41 — — 11
899	317 3 —	929	3 — 317	959	353 329	989	313 319
900	— 3 — 3	930	71 341 3	960	— 313 3	990	— 3 — 3
901	— — 71 29	931	— 67 7 —	961	7 — 59 —	991	11 23 47 7
902	3 7 3 —	932	3 — 319	962	3 — 3 —	992	3 — 3 —
903	11 3 7 3	933	7 3 — 3	963	— 323 3	993	— 319 3
904	— — 83 —	934	— — 13 —	964	31 — 11 —	994	— 61 7 —
905	311 3 —	935	347 3 7	965	3 7 313	995	337 323
906	13 3 3	936	11 317 3	966	— 3 7 3	996	7 3 — 3
907	47 43 29 7	937	— 7 — 83	967	19 17 — —	997	13 — 11 17
908	331 361	938	311 341	968	323 3 —	998	367 3 7
909	— 311 3	939	— 3 — 3	969	11 3 — 3	999	97 313 3

表B 200,000以内的平方数表

	0	1	2	3	4	5	6	7	8	9
0	0	1	4	9	16	25	36	49	64	81
1	100	121	144	169	196	225	256	289	324	361
2	400	441	484	529	576	625	676	729	784	841
3	900	961	1024	1089	1156	1225	1296	1369	1444	1521
4	1600	1681	1764	1849	1936	2025	2116	2209	2304	2401
5	2500	2601	2704	2809	2916	3025	3136	3249	3364	3481
6	3600	3721	3844	3969	4096	4225	4356	4489	4624	4761
7	4900	5041	5184	5329	5476	5625	5776	5929	6084	6241
8	6400	6561	6724	6889	7056	7225	7396	7569	7744	7921
9	8100	8281	8464	8649	8836	9025	9216	9409	9604	9801
10	10000	10201	10404	10609	10816	11025	11236	11449	11664	11881
11	12100	12321	12544	12769	12996	13225	13456	13689	13924	14161
12	14400	14641	14884	15129	15376	15625	15876	16129	16384	16641
13	16900	17161	17424	17689	17956	18225	18496	18769	19044	19321
14	19600	19881	20164	20449	20736	21025	21316	21609	21904	22201
15	22500	22801	23104	23409	23716	24025	24336	24649	24964	25281
16	25600	25921	26244	26569	26896	27225	27556	27889	28224	28561
17	28900	29241	29584	29929	30276	30625	30976	31329	31684	32041
18	32400	32761	33124	33489	33856	34225	34596	34969	35344	35721
19	36100	36481	36864	37249	37636	38025	38416	38809	39204	39601

20	40000	40401	40804	41209	41616	42025	42436	42849	43264	43681
21	44100	44521	44944	45369	45796	46225	46656	47089	47524	47961
22	48400	48841	49284	49729	50176	50625	51076	51529	51984	52441
23	52900	53361	53824	54289	54756	55225	55696	56169	56644	57121
24	57600	58081	58564	59049	59536	60025	60516	61009	61504	62001
25	62500	63001	63504	64009	64516	65025	65536	66049	66564	67081
26	67600	68121	68644	69169	69696	70225	70756	71289	71824	72361
27	72900	73441	73984	74529	75076	75625	76176	76729	77284	77841
28	78400	78961	79524	80089	80656	81225	81796	82369	82944	83521
29	84100	84681	85264	85849	86436	87025	87616	88209	88804	89401
30	90000	90601	91204	91809	92416	93025	93636	94249	94864	95481
31	96100	96721	97344	97969	98596	99225	99856	100489	101124	101761
32	102400	103041	103684	104329	104976	105625	106276	106929	107584	108241
33	108900	109561	110224	110889	111556	112225	112896	113569	114244	114921
34	115600	116281	116964	117649	118336	119025	119716	120409	121104	121801
35	122500	123201	123904	124609	125316	126025	126736	127449	128164	128881
36	129600	130321	131044	131769	132496	133225	133956	134689	135424	136161
37	136900	137641	138384	139129	139876	140625	141376	142129	142884	143641
38	144400	145161	145924	146689	147456	148225	148996	149769	150544	151321
39	152100	152881	153664	154449	155236	156025	156816	157609	158404	159201
40	160000	160801	161604	162409	163216	164025	164836	165649	166464	167281
41	168100	168921	169744	170569	171396	172225	173056	173889	174724	175561
42	176400	177241	178084	178929	179776	180625	181476	182329	183184	184041
43	184900	185761	186624	187489	188356	189225	190096	190969	191844	192721
44	193600	194481	195364	196249	197136	198025	198916	199809		

上页表列出了 200,000 以内的所有平方数，这些数是整数 $n(0\leqslant n\leqslant 447)$ 的平方. 要在表中查到 n^2，可看一下 n 的个位数开头的那一列和 $[n/10]$ 所在的那一行的交点处的数. 例如，314^2 位于 31 所在行和以 4 开头的那一列：$314^2=98,596$.

表 C 部分整数的因子分解表

下表给出了整数 n 的素数幂分解式，n 的范围是：$10,000\leqslant n\leqslant 10,269$；$100,000\leqslant n\leqslant 100,149$.

10000	$2^4\cdot5^4$	10030	$2\cdot5\cdot17\cdot59$	10060	$2^2\cdot5\cdot503$
10001	$73\cdot137$	10031	$7\cdot1433$	10061	10061
10002	$2\cdot3\cdot1667$	10032	$2^4\cdot3\cdot11\cdot19$	10062	$2\cdot3^2\cdot13\cdot43$
10003	$7\cdot1429$	10033	$79\cdot127$	10063	$29\cdot347$
10004	$2^2\cdot41\cdot61$	10034	$2\cdot29\cdot173$	10064	$2^4\cdot17\cdot37$
10005	$3\cdot5\cdot23\cdot29$	10035	$3^2\cdot5\cdot223$	10065	$3\cdot5\cdot11\cdot61$
10006	$2\cdot5003$	10036	$2^2\cdot13\cdot193$	10066	$2\cdot7\cdot719$
10007	10007	10037	10037	10067	10067
10008	$2^3\cdot3^2\cdot139$	10038	$2\cdot3\cdot7\cdot239$	10068	$2^2\cdot3\cdot839$
10009	10009	10039	10039	10069	10069
10010	$2\cdot5\cdot7\cdot11\cdot13$	10040	$2^3\cdot5\cdot251$	10070	$2\cdot5\cdot19\cdot53$
10011	$3\cdot47\cdot71$	10041	$3\cdot3347$	10071	$3^3\cdot373$
10012	$2^2\cdot2503$	10042	$2\cdot5021$	10072	$2^3\cdot1259$
10013	$17\cdot19\cdot31$	10043	$11^2\cdot83$	10073	$7\cdot1439$
10014	$2\cdot3\cdot1669$	10044	$2^2\cdot3^4\cdot31$	10074	$2\cdot3\cdot23\cdot73$
10015	$5\cdot2003$	10045	$5\cdot7^2\cdot41$	10075	$5^2\cdot13\cdot31$
10016	$2^5\cdot313$	10046	$2\cdot5023$	10076	$2^2\cdot11\cdot229$
10017	$3^3\cdot7\cdot53$	10047	$3\cdot17\cdot197$	10077	$3\cdot3359$
10018	$2\cdot5009$	10048	$2^6\cdot157$	10078	$2\cdot5039$
10019	$43\cdot233$	10049	$13\cdot773$	10079	10079
10020	$2^2\cdot3\cdot5\cdot167$	10050	$2\cdot3\cdot5^2\cdot67$	10080	$2^5\cdot3^2\cdot5\cdot7$
10021	$11\cdot911$	10051	$19\cdot23^2$	10081	$17\cdot593$
10022	$2\cdot5011$	10052	$2^2\cdot7\cdot359$	10082	$2\cdot71^2$
10023	$3\cdot13\cdot257$	10053	$3^2\cdot1117$	10083	$3\cdot3361$
10024	$2^3\cdot7\cdot179$	10054	$2\cdot11\cdot457$	10084	$2^2\cdot2521$
10025	$5^2\cdot401$	10055	$5\cdot2011$	10085	$5\cdot2017$
10026	$2\cdot3^2\cdot557$	10056	$2^3\cdot3\cdot419$	10086	$2\cdot3\cdot41^2$
10027	$37\cdot271$	10057	$89\cdot113$	10087	$7\cdot11\cdot131$
10028	$2^2\cdot23\cdot109$	10058	$2\cdot47\cdot107$	10088	$2^3\cdot13\cdot97$
10029	$3\cdot3343$	10059	$3\cdot7\cdot479$	10089	$3^2\cdot19\cdot59$

10090	$2\cdot5\cdot1009$
10091	10091
10092	$2^2\cdot3\cdot29^2$
10093	10093
10094	$2\cdot7^2\cdot103$
10095	$3\cdot5\cdot673$
10096	$2^4\cdot631$
10097	$23\cdot439$
10098	$2\cdot3^3\cdot11\cdot17$
10099	10099
10100	$2^2\cdot5^2\cdot101$
10101	$3\cdot7\cdot13\cdot37$
10102	$2\cdot5051$
10103	10103
10104	$2^3\cdot3\cdot421$
10105	$5\cdot43\cdot47$
10106	$2\cdot31\cdot163$
10107	$3^2\cdot1123$
10108	$2^2\cdot7\cdot19^2$
10109	$11\cdot919$
10110	$2\cdot3\cdot5\cdot337$
10111	10111
10112	$2^7\cdot79$
10113	$3\cdot3371$
10114	$2\cdot13\cdot389$
10115	$5\cdot7\cdot17^2$
10116	$2^2\cdot3^2\cdot281$
10117	$67\cdot151$
10118	$2\cdot5059$
10119	$3\cdot3373$
10120	$2^3\cdot5\cdot11\cdot23$
10121	$29\cdot349$
10122	$2\cdot3\cdot7\cdot241$
10123	$53\cdot191$
10124	$2^2\cdot2531$
10125	$3^4\cdot5^3$
10126	$2\cdot61\cdot83$
10127	$13\cdot19\cdot41$
10128	$2^4\cdot3\cdot211$
10129	$7\cdot1447$
10130	$2\cdot5\cdot1013$
10131	$3\cdot11\cdot307$
10132	$2^2\cdot17\cdot149$
10133	10133
10134	$2\cdot3^2\cdot563$
10135	$5\cdot2027$
10136	$2^3\cdot7\cdot181$
10137	$3\cdot31\cdot109$
10138	$2\cdot37\cdot137$
10139	10139
10140	$2^2\cdot3\cdot5\cdot13^2$
10141	10141
10142	$2\cdot11\cdot461$
10143	$3^2\cdot7^2\cdot23$
10144	$2^5\cdot317$
10145	$5\cdot2029$
10146	$2\cdot3\cdot19\cdot89$
10147	$73\cdot139$
10148	$2^2\cdot43\cdot59$
10149	$3\cdot17\cdot199$
10150	$2\cdot5^2\cdot7\cdot29$
10151	10151
10152	$2^3\cdot3^3\cdot47$
10153	$11\cdot13\cdot71$
10154	$2\cdot5077$
10155	$3\cdot5\cdot677$
10156	$2^2\cdot2539$
10157	$7\cdot1451$
10158	$2\cdot3\cdot1693$
10159	10159
10160	$2^4\cdot5\cdot127$
10161	$3^2\cdot1129$
10162	$2\cdot5081$
10163	10163
10164	$2^2\cdot3\cdot7\cdot11^2$
10165	$5\cdot19\cdot107$
10166	$2\cdot13\cdot17\cdot23$
10167	$3\cdot3389$
10168	$2^3\cdot31\cdot41$
10169	10169
10170	$2\cdot3^2\cdot5\cdot113$
10171	$7\cdot1453$
10172	$2^2\cdot2543$
10173	$3\cdot3391$
10174	$2\cdot5087$
10175	$5^2\cdot11\cdot37$
10176	$2^6\cdot3\cdot53$
10177	10177
10178	$2\cdot7\cdot727$
10179	$3^3\cdot13\cdot29$
10180	$2^2\cdot5\cdot509$
10181	10181
10182	$2\cdot3\cdot1697$
10183	$17\cdot599$
10184	$2^3\cdot19\cdot67$
10185	$3\cdot5\cdot7\cdot97$
10186	$2\cdot11\cdot463$
10187	$61\cdot167$
10188	$2^2\cdot3^2\cdot283$
10189	$23\cdot443$
10190	$2\cdot5\cdot1019$
10191	$3\cdot43\cdot79$
10192	$2^4\cdot7^2\cdot13$
10193	10193
10194	$2\cdot3\cdot1699$
10195	$5\cdot2039$
10196	$2^2\cdot2549$
10197	$3^2\cdot11\cdot103$
10198	$2\cdot5099$
10199	$7\cdot31\cdot47$
10200	$2^3\cdot3\cdot5^2\cdot17$
10201	101^2
10202	$2\cdot5101$
10203	$3\cdot19\cdot179$
10204	$2^2\cdot2551$
10205	$5\cdot13\cdot157$
10206	$2\cdot3^6\cdot7$
10207	$59\cdot173$
10208	$2^5\cdot11\cdot29$
10209	$3\cdot41\cdot83$

10210	$2\cdot5\cdot1021$	10230	$2\cdot3\cdot5\cdot11\cdot31$	10250	$2\cdot5^3\cdot41$
10211	10211	10231	$13\cdot787$	10251	$3^2\cdot17\cdot67$
10212	$2^2\cdot3\cdot23\cdot37$	10232	$2^3\cdot1279$	10252	$2^2\cdot11\cdot233$
10213	$7\cdot1459$	10233	$3^3\cdot379$	10253	10253
10214	$2\cdot5107$	10234	$2\cdot7\cdot17\cdot43$	10254	$2\cdot3\cdot1709$
10215	$3^2\cdot5\cdot227$	10235	$5\cdot23\cdot89$	10255	$5\cdot7\cdot293$
10216	$2^3\cdot1277$	10236	$2^2\cdot3\cdot853$	10256	$2^4\cdot641$
10217	$17\cdot601$	10237	$29\cdot353$	10257	$3\cdot13\cdot263$
10218	$2\cdot3\cdot13\cdot131$	10238	$2\cdot5119$	10258	$2\cdot23\cdot223$
10219	$11\cdot929$	10239	$3\cdot3413$	10259	10259
10220	$2^2\cdot5\cdot7\cdot73$	10240	$2^{11}\cdot5$	10260	$2^2\cdot3^3\cdot5\cdot19$
10221	$3\cdot3407$	10241	$7^2\cdot11\cdot19$	10261	$31\cdot331$
10222	$2\cdot19\cdot269$	10242	$2\cdot3^2\cdot569$	10262	$2\cdot7\cdot733$
10223	10223	10243	10243	10263	$3\cdot11\cdot311$
10224	$2^4\cdot3^2\cdot71$	10244	$2^2\cdot13\cdot197$	10264	$2^3\cdot1283$
10225	$5^2\cdot409$	10245	$3\cdot5\cdot683$	10265	$5\cdot2053$
10226	$2\cdot5113$	10246	$2\cdot47\cdot109$	10266	$2\cdot3\cdot29\cdot59$
10227	$3\cdot7\cdot487$	10247	10247	10267	10267
10228	$2^2\cdot2557$	10248	$2^3\cdot3\cdot7\cdot61$	10268	$2^2\cdot17\cdot151$
10229	$53\cdot193$	10249	$37\cdot277$	10269	$3^2\cdot7\cdot163$

100000	$2^5\cdot5^5$	100020	$2^2\cdot3\cdot5\cdot1667$	100040	$2^3\cdot5\cdot41\cdot61$
100001	$11\cdot9091$	100021	$29\cdot3449$	100041	$3\cdot33347$
100002	$2\cdot3\cdot7\cdot2381$	100022	$2\cdot13\cdot3847$	100042	$2\cdot50021$
100003	100003	100023	$3\cdot7\cdot11\cdot433$	100043	100043
100004	$2^2\cdot23\cdot1087$	100024	$2^3\cdot12503$	100044	$2^2\cdot3^2\cdot7\cdot397$
100005	$3\cdot5\cdot59\cdot113$	100025	$5^2\cdot4001$	100045	$5\cdot11\cdot17\cdot107$
100006	$2\cdot31\cdot1613$	100026	$2\cdot3^2\cdot5557$	100046	$2\cdot50023$
100007	$97\cdot1031$	100027	$23\cdot4349$	100047	$3\cdot33349$
100008	$2^3\cdot3^3\cdot463$	100028	$2^2\cdot17\cdot1471$	100048	$2^4\cdot13^2\cdot37$
100009	$7^2\cdot13\cdot157$	100029	$3\cdot33343$	100049	100049
100010	$2\cdot5\cdot73\cdot137$	100030	$2\cdot5\cdot7\cdot1429$	100050	$2\cdot3\cdot5^2\cdot23\cdot29$
100011	$3\cdot17\cdot37\cdot53$	100031	$67\cdot1493$	100051	$7\cdot14293$
100012	$2^2\cdot11\cdot2273$	100032	$2^6\cdot3\cdot521$	100052	$2^2\cdot25013$
100013	$103\cdot971$	100033	$167\cdot599$	100053	$3^2\cdot11117$
100014	$2\cdot3\cdot79\cdot211$	100034	$2\cdot11\cdot4547$	100054	$2\cdot19\cdot2633$
100015	$5\cdot83\cdot241$	100035	$3^4\cdot5\cdot13\cdot19$	100055	$5\cdot20011$
100016	$2^4\cdot7\cdot19\cdot47$	100036	$2^2\cdot89\cdot281$	100056	$2^3\cdot3\cdot11\cdot379$
100017	$3^2\cdot11113$	100037	$7\cdot31\cdot461$	100057	100057
100018	$2\cdot43\cdot1163$	100038	$2\cdot3\cdot16673$	100058	$2\cdot7^2\cdot1021$
100019	100019	100039	$71\cdot1409$	100059	$3\cdot33353$

100060	$2^2 \cdot 5 \cdot 5003$	100090	$2 \cdot 5 \cdot 10009$	100120	$2^3 \cdot 5 \cdot 2503$
100061	$13 \cdot 43 \cdot 179$	100091	$101 \cdot 991$	100121	$7 \cdot 14303$
100062	$2 \cdot 3^3 \cdot 17 \cdot 109$	100092	$2^2 \cdot 3 \cdot 19 \cdot 439$	100122	$2 \cdot 3 \cdot 11 \cdot 37 \cdot 41$
100063	$47 \cdot 2129$	100093	$7 \cdot 79 \cdot 181$	100123	$59 \cdot 1697$
100064	$2^5 \cdot 53 \cdot 59$	100094	$2 \cdot 50047$	100124	$2^2 \cdot 25031$
100065	$3 \cdot 5 \cdot 7 \cdot 953$	100095	$3 \cdot 5 \cdot 6673$	100125	$3^2 \cdot 5^3 \cdot 89$
100066	$2 \cdot 50033$	100096	$2^8 \cdot 17 \cdot 23$	100126	$2 \cdot 13 \cdot 3851$
100067	$11^2 \cdot 827$	100097	$199 \cdot 503$	100127	$223 \cdot 449$
100068	$2^2 \cdot 3 \cdot 31 \cdot 269$	100098	$2 \cdot 3^2 \cdot 67 \cdot 83$	100128	$2^5 \cdot 3 \cdot 7 \cdot 149$
100069	100069	100099	$31 \cdot 3229$	100129	100129
100070	$2 \cdot 5 \cdot 10007$	100100	$2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	100130	$2 \cdot 5 \cdot 17 \cdot 19 \cdot 31$
100071	$3^2 \cdot 11119$	100101	$3 \cdot 61 \cdot 547$	100131	$3 \cdot 33377$
100072	$2^3 \cdot 7 \cdot 1787$	100102	$2 \cdot 50051$	100132	$2^2 \cdot 25033$
100073	$19 \cdot 23 \cdot 229$	100103	100103	100133	$11 \cdot 9103$
100074	$2 \cdot 3 \cdot 13 \cdot 1283$	100104	$2^3 \cdot 3 \cdot 43 \cdot 97$	100134	$2 \cdot 3^2 \cdot 5563$
100075	$5^2 \cdot 4003$	100105	$5 \cdot 20021$	100135	$5 \cdot 7 \cdot 2861$
100076	$2^2 \cdot 127 \cdot 197$	100106	$2 \cdot 50053$	100136	$2^3 \cdot 12517$
100077	$3 \cdot 33359$	100107	$3^2 \cdot 7^2 \cdot 227$	100137	$3 \cdot 29 \cdot 1151$
100078	$2 \cdot 11 \cdot 4549$	100108	$2^2 \cdot 29 \cdot 863$	100138	$2 \cdot 50069$
100079	$7 \cdot 17 \cdot 29^2$	100109	100109	100139	$13 \cdot 7703$
100080	$2^4 \cdot 3^2 \cdot 5 \cdot 139$	100110	$2 \cdot 3 \cdot 5 \cdot 47 \cdot 71$	100140	$2^2 \cdot 3 \cdot 5 \cdot 1669$
100081	$41 \cdot 2441$	100111	$11 \cdot 19 \cdot 479$	100141	$239 \cdot 419$
100082	$2 \cdot 163 \cdot 307$	100112	$2^4 \cdot 6257$	100142	$2 \cdot 7 \cdot 23 \cdot 311$
100083	$3 \cdot 73 \cdot 457$	100113	$3 \cdot 13 \cdot 17 \cdot 151$	100143	$3^3 \cdot 3709$
100084	$2^2 \cdot 131 \cdot 191$	100114	$2 \cdot 7 \cdot 7151$	100144	$2^4 \cdot 11 \cdot 569$
100085	$5 \cdot 37 \cdot 541$	100115	$5 \cdot 20023$	100145	$5 \cdot 20029$
100086	$2 \cdot 3 \cdot 7 \cdot 2383$	100116	$2^2 \cdot 3^5 \cdot 103$	100146	$2 \cdot 3 \cdot 16691$
100087	$13 \cdot 7699$	100117	$53 \cdot 1889$	100147	$17 \cdot 43 \cdot 137$
100088	$2^3 \cdot 12511$	100118	$2 \cdot 113 \cdot 443$	100148	$2^2 \cdot 25037$
100089	$3^3 \cdot 11 \cdot 337$	100119	$3 \cdot 23 \cdot 1451$	100149	$3 \cdot 7 \cdot 19 \cdot 251$

练 习 答 案

§1

1. 所有整数.

4. 2, 5, 2.

5. 1, n.

6. d.

7. 3, 3;3, 0.

9. 13, 34.

10. $x=5$, $y=-6$.

§2

1. 一个,一个.

3. $72=2^3\cdot 3^2$, $480=2^5\cdot 3\cdot 5$.

4. 对某n, 有$p|a_n$.

5. 假设$k=r-1$时,结论成立,则由$p|(a_1a_2\cdots a_{r-1})a_r$知,$p|a_1a_2\cdots a_{r-1}$或$p|a_r$. 在第一种情况下, 根据归纳法假设, 知对某$j(1\leqslant j\leqslant r-1)$, 有$p|a_j$; 在第二种情况下, $p|a_r$. 无论是哪种情况, 都有$p|a_j$, 其中j是满足$1\leqslant j\leqslant r$之某数, 故结论对$k=r$也成立. 又结论对$k=1$是成立的,故它对一切k都成立.

6. 25, 45, 65, 81, 85.

7. $2\cdot 3\cdot 5^2\cdot 53$.

§3

1. 左端是偶数;右端是奇数.

2. 所有的解为: $x=5t$, $y=2-t$, 其中t是整数.

3. (c).

4. $x=10+3t$, $y=-t$, t为整数.

5. $x=6$, $y=1$; $x=3$, $y=2$.

§ 4

1. 真,真,假,真.

2. 则有 $km=a-b$,故 $m|(a-b)$, $a\equiv b(\bmod m)$.

3. 1, 7, 9, 4, 8.

4. $n\equiv1(\bmod 2)$. 对某 k 有, $n=1+2k$. n 用 2 相除时,余数为 1.

9. 例如, $5\cdot4\equiv5\cdot6(\bmod 10)$, 但 $4\not\equiv6(\bmod 10)$.

10. (a)$x\equiv2(\bmod 7)$; (b)$x\equiv4(\bmod 7)$.

11. $x\equiv2(\bmod 3)$.

12. 两式都错.

§ 5

1. 例如, $4x\equiv3$, $5x\equiv4$, $6x\equiv6(\bmod 12)$分别为无解,有一解,有六解.

2. (b), (c), (d)都无解.

3. 就是定理 1 中的结论.

4. (a)2; (b)$x=-1+10t$, $y=2-9t$.

5. 3, 1, 5, 0, 1.

6. $x=2$, 5, 8, 11, 14.

7. 2, 7, 12; 2; 无解; 2.

9. 任何 $x\equiv104(\bmod 105)$.

§ 6

2. 10, 1.

3. (2, 6), (3, 4), (5, 9), (7, 8).

§ 7

1.

n	11	12	13	14	15	16
$d(n)$	2	6	2	4	4	5.

2. $d(p^3)=4$. $d(p^n)=n+1$.

3. $d(p^3q)=8$. $d(p^nq)=2(n+1)$.

4. 20.

5.

n	9	10	11	12	13	14
$\sigma(n)$	13	18	12	28	14	24.

6. $\sigma(p^3)=1+p+p^2+p^3$. $\sigma(pq)=1+p+q+pq$.

8. $\sigma(p^n)=1+p+p^2+\cdots+p^n=(p^{n+1}-1)/(p-1)$.

9. $\sigma(240)=744$.

10.

n	13	14	15	16	17	18	19	20	21	22	23	24
$f(n)$	1	1	1	32	1	6	1	4	1	1	1	12

§ **9**

5. 1, 3. 1, 3, 5, 7. 1, 3, 5, 7, 9, 11, 13, 15.
   $\phi(2^n)=2^{n-1}$ 是小于 2^n 的正奇数个数.

7. $\phi(m)$.

8. 24, 36, 36.

9. (a)12, 13, 14, 15, 16; (b)2^k; (c)p^k.

10. $C_1=\{1, 3, 5, 9, 11, 13\}$, $C_2=\{2, 4, 6, 8, 10, 12\}$, $C_7=\{7\}$, $C_{14}=\{14\}$.

§ **10**

1. 2, 2, 2.

2. 1, 2, 3, 6. 2 和 5 的阶为 6, 4 和 7 的阶为 3; 8 的阶为 2, 1 的阶为 1.

3. 191(39, 77, 115, 153 都是合数).

5. 3 和 7 是 10 的原根.

6. 其阶分别为 2, 4, 1.

8. 8, 12, 15, 16, 20, 21, 24.

9. 对模 7 有: $\mathrm{ind}_5 1=0$, $\mathrm{ind}_5 2=4$, $\mathrm{ind}_5 3=5$, $\mathrm{ind}_5 4=2$, $\mathrm{ind}_5 5=1$, $\mathrm{ind}_5 6=3$.

§ **11**

1. $x^2+4x+3\equiv 0 \pmod 5$.

2. $(x+2)^2\equiv 1 \pmod 5$.

3. 2 和 4.

4. 2 和 $p-2$.

5. 1, 3, 4, 5, 9.

6. 15 和 16.

7. 1, 1, 1, 1.

8. 1, 1, 1.

9. 若 $p\nmid a$, 则 $(a^2/p)=1$.

13. 1, 1.

14. 5, 13, 17.

15. −1, −1.

§ 12

2. 无解.

7. 它们全非奇素数.

§ 13

1. $31=2^4+2^3+2^2+2^1+2^0$. $33=2^5+2^0$.

2. 6, 7.

3. $n'<2^r$. 因此对一切 i, 有 $r>e_i$.

4. 9, 7, 64.

5. 10_2, 10100_2, 11001000_2.

§ 14

1. 11, 19, 110, 6χ.

3. 28, 40, $6\chi6$.

4. 8.

5. 371, 275.

§ 15

1. 73/4950.

2. $0.\overline{17073}$.

3. 4, 2, 2.

4. 7, 6, 5.

5. $0.\overline{02439}$.

6. 5.

§ 16

1. 若 p 整除 x, y, z 中任意两数,则它也必整除另一数.

2. 否则, 2 就会整除 (a, b).

§ 17

1. $c^2\equiv 2 \pmod 4$ 是不可能成立的.

6. (a) 因为 $n=2v^2$; (b) 因为 $b^2=m^2-n^2$.

7. 若 $n=0$, 则 $a^2=2mn=0$, a, b, c 就是一组平凡解.

§ 18

2. $325=18^2+1^2$.

4. 若 $r=s=0$, 则 $k|x$, $k|y$. 因而 $k|p$, 就有 $k=1$ 或 $k=p$. 我们在开始时已假定 $k>1$. 若 $k=p$, 则 x 和 y 中有一为零,得出矛盾.

§ 19

1. $3\cdot 17=7^2+1^2+1^2+0^2=5^2+4^2+3^2+1^2$.

§ 20

1. 最小解为 $3^2-2\cdot 2^2=1$ 和 $2^2-3\cdot 1^2=1$.

2. 若 $x-my=x+my=1$, 则 $2x=2$. 另一情况与此相似.

3. 26, 15.

4. $(r+sN^{1/2})^k(r-sN^{1/2})^k=(r^2-Ns^2)^k=1^k=1$.

§ 21

1. 若 $(a, b)=d$, 则对所有 n, $d|(an+b)$, 此序列至多只包含一个素数,即 d 本身(如果 d 是素数的话).

3. 检验 mod 2, mod 3, mod 7 这几种情况.

5. 检验各种情况,或利用 $n^2+21n+1\equiv(n+1)^2 \pmod{19}$.

§ 22

1. 4, 5, 2, 2.

4. $\psi(32)=\log(2^4\cdot 3^3\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29)=28.5\cdots$.

5. 在第 m 列中,共有 $[x/2^m]$ 个非零项.

6. $\theta((x/2)^{1/m})$, 其中 $m=[\log(x/2)/\log 2]$. $\theta((x/m)^{1/2})$, 其中 $m=[x/2^2]$.

7. 是;最后一项为$[x/p^m]$,其中 $m=[\log x/\log p]$.

9. $[\log n/\log p]$.

10. 110.

13. $n=[\log x/\log 2]$.

附录一

1. $f(n)=(n-1)^2$.

2. $f(n)=n^2+1$.

3. $f(n)=n^2-6n+7$.

4. 所有 $n\geqslant 17$.

5. “$1=1\cdot 2/2$”. 是.

附录二

1. (a) $f(1)g(6)+f(2)g(5)+f(3)g(4)+f(4)g(3)+f(5)g(2)+f(6)g(1)$;

   (b) $\phi(1)+\phi(2)/2+\phi(3)/3$;

   (c) $f(2)g(-1)+f(3)g(-1)+f(4)g(-1)+f(2)g(0)+f(3)g(0)+f(4)g(0)+f(2)g(1)+f(3)g(1)+f(4)g(1)$.

2. (a) $\sum_{i=1}^{k} i$; (b) $\sum_{j=1}^{17} j/(2j+1)$; (c) $\sum_{k=2}^{17} k/(k-1)^2$. 这些和式也可以有其它正确的记法.

3. (a) 2; (b) 2; (c) 24.

4. (a) 41; (b) 45; (c) 9801.

5. (a) 1; (b) 2^{17}; (c) 3/14.

6. 对任何整数 n, 有 $[x+n]=[x]+n$.

8. 179.

附录三

2. 13 或 68.

3. 13, 122.

4. 23, 41, 87, 或 105.

6. 23, 41, 55.

7. 无解, 因为不可能成立 $x^2\equiv 10 \pmod{16}$.

习 题 提 示

§ 1

2. 若 $a=k_1b$, $b=k_2a$, 则 $k_1k_2=1$, 故 $k_1=k_2=1$ 或 $k_1=k_2=-1$.

4. 利用题 3.

6. (b) 若 $d|n$, $d|(n+2)$, 则 $d|2$.

7. 若 $d|n_i$, $d|N$, 则 $d|(N-n_1n_2\cdots n_k)$.

8. 若 $d>0$, $d|c$, $d|b$, 则 $d|a$, $d|b$.

10. (b) 若 $d|k$, $d|(n+k)$, 则 $d|n$. 或用引理 4.

11. (b) 若 $299r+247s=13$, 则 $299(r+247)+247(s-299)=13$.

12. (b) 若 r/s 为一根,则 $(r/s)^2+a(r/s)+b=0$, 或 $r^2+ars+bs^2=0$. 利用定理 4 证明: 若 $s|r^2$, $(r, s)=1$, 则 $s|1$.

15. $(c/d, a/d)=1$, $(c/d)|(a/d)b$; 应用定理 5.

16. 先证 $d|2a$ 和 $d|2b$, 再应用定理 6.

19. 或者使用归纳法, 或者先证明: 任意三个相继整数中, 必有一个被 2 整除, 一个被 3 整除.

20. (a) 若 3^m 的最后一位数为 9, 则 $3^m(81)^n$ 的最后一位数也为 9.

§ 2

1. (f) $111|111,111$;

   (g) 注意, $10^{12}-1=(10^2-1)(10^2+1)(10^4-10^2+1)(10^4+10^2+1)$ $=99\cdot101\cdot9901\cdot10101$. 利用表 A 和表 C.

4. (b) 一种方法是: 设 $n=20+77k$, $k=0, 1, \cdots$, 则对所有 n, 有 $7|(6n-1)$, $11|(6n+1)$.

9. 一种方法是: 用题 6 和题 8 证明 n 和 $n+1$ 必须都是平方数.

11. 写出 $17p=n^2-1=(n+1)(n-1)$, 并考虑下列几种情况: $17=n-1$, $n+1$, n^2-1.

13. 验证: $2^{ab}-1=(2^a-1)(2^{(b-1)a}+2^{(b-2)a}+\cdots+1)$.

15. $n/p<n^{2/3}$. 若 n/p 为合数，它就有一个比 $(n^{2/3})^{1/2}=n^{1/3}$ 还要小的素因子，得出矛盾。

19. (a) $N+((N-1)/2)^2=((N+1)/2)^2$.

20. 假定 n 是合数，那么 $p_1, p_2, \cdots, p_k$ 中必有 n 的一个素因子。

22. 若 $p|a_i$, $p|a_j(i\neq j)$, 则 $p|(a_i-a_j)$, 故 $p|(i-j)P_n$. 因 $p|a_i$, 故 $p|P_n$ 是不可能的；$p|(i-j)$ 也不可能，因为 $-n\leqslant i-j\leqslant n$, 而由 $p|a_i$, 必有 $p\geqslant p_n>n$.

§ 4

8. 用“弃九法”。

10. 每一整数必与 $0^2, 1^2, 2^2, \cdots, 9^2$ 中的一个数同余 (mod 10)。

13. $(n+1)^3-n^3=3n(n+1)+1$.

14. 当 $n\equiv 0, 1, 2, 3, 4 \pmod 5$ 时，考虑 $3n^2+3n+1$.

15. 证明：$d_k 10^k+d_{k-1}10^{k-1}+\cdots+d_0\equiv d_k+d_{k-1}+\cdots+d_0 \pmod 3$.

18. 只要证明：由 $a_i\equiv a_j \pmod p$, 可得 $i=j$.

19. 一个闰年的二月一日与下一个闰年的二月一日间有 $3\cdot 365+366=1461$ 天，$1461\equiv 5 \pmod 7$. 记住，公元 2000 年将是闰年。

20. 形如 $abba$ 的数与 $a-b+b-a$ 同余 (mod 11)。

23. 证明：任何立方数与 0, 1, 8 三数中一数同余 (mod 9)，而在这些数中，任选三个数相加都不会与 4 同余 (mod 9)。

24. 写出 $x^m-1=(x-1)(x^{m-1}+x^{m-2}+\cdots+1)$, 并说明 $m^k|(x-1)$ 和 $m|(x^{m-1}+x^{m-2}+\cdots+1)$.

25. $7\cdot 11\cdot 13=1001$. 证明 $n\equiv f(n) \pmod{1001}$, 因而，若 7, 11, 13 三数中任一数整除 $f(n)$, 则它也整除 n.

§ 5

1. (e) 由表 A, $6191=41\cdot 151$, 故该同余式等价于 $40x\equiv 191 \pmod{41}$ 和 $40x\equiv 191 \pmod{151}$. 因此，$x\equiv 14 \pmod{41}$, $x\equiv 1 \pmod{151}$.

4. (d) 该同余式组即为

$$x\equiv 3 \pmod 5,\ x\equiv 3 \pmod 7,\ x\equiv 3 \pmod{11}.$$

5. 将 2401 的倍数逐个加于 4, 直至得到 9 的倍数为止。

7. 解同余式组：$n\equiv 0 \pmod 3$, $n\equiv 3 \pmod 5$, $n\equiv 3 \pmod 7$.

8. 设此数为 $2^a 3^b 5^c$, 求 a, b, c 应满足的条件。

9. 注意，由 $x\equiv1 \pmod 6$ 便必有 $x\equiv1 \pmod 2$ 和 $x\equiv1 \pmod 3$，故后两个条件是多余的.

10. (b) $n=4k_1$ 和 $n=16k_2-2$. 不可能成立 $4k_1\equiv16k_2-2 \pmod 4$.

11. 我们知道，对于某 k_1 和 k_2，有

$$(m+1)x=r(m+1)+k_1m(m+1),$$
$$mx=sm+k_2m(m+1),$$

再将两式相减.

13. 求解 $3a=20r+r,$
$5b=20(r+1)+(r+1),$
$7c=20(r+2)+(r+2).$

17. 应用定理 1

§ **6**

2. 163 是素数.

3. $7^4\equiv1 \pmod{10}$.

4. $7^4\equiv1 \pmod{100}$.

7. $-1\equiv(p-1)!\equiv(p-k)!(p-(k-1))(p-(k-2))\cdots(p-1) \pmod p$，以及 $p-r\equiv-r \pmod p$.

9. $(p-1)!=(p-1)(p-2)(p-3)!$.

10. 利用题 5.

11. (a) 应用二项式公式（参见附录二），我们有

$$(k+1)^p=k^p+\binom{p}{1}k^{p-1}+\binom{p}{2}k^{p-2}+\cdots+\binom{p}{p-1}k+1,$$

且对 $r=1, 2, \cdots, p-1$，有 $p\left|\binom{p}{r}\right.$.

(b) 使用归纳法，或者将下列各同余式相加:

$$1^p-0^p\equiv1 \pmod p,$$
$$2^p-1^p\equiv1 \pmod p,$$
$$\cdots$$
$$a^p-(a-1)^p\equiv1 \pmod p.$$

12. 由费马定理知，$a^n\equiv b^n\equiv1 \pmod{n+1}$.

13. (b) $1+2+\cdots+(p-1)=p(p-1)/2$;

(c) $2, 4, 6, \cdots, 2(p-1)$的最小剩余$(\bmod p)$是$1, 2, \cdots, p-1$的一个排列，故有

$$1^m+2^m+\cdots+(p-1)^m\equiv 2^m+4^m+\cdots+(2(p-1))^m(\bmod p),$$

即有
$$\sum_{i=1}^{p-1} i^m\equiv 2^m\sum_{i=1}^{p-1} i^m(\bmod p);$$

因$2^m\not\equiv 1(\bmod p)$，我们有$p\mid\sum_{i=1}^{p-1} i^m$.

14. 关于威尔逊定理，可令$a=1$. 而要得到费马定理，我们有$a^p(-1)\equiv a(-1)(\bmod p)$.

17. 证明$11^{341}-11=13(\bmod 31)$.

18. (a) $a^{p+q}-a^{p+1}-a^{q+1}+a^2=(a^p-a)(a^q-a)$;

(b) $a^{pq}-a^p\equiv a^q-a(\bmod p)$，且$a^{pq}-a^q=a^p-a(\bmod q)$.

19. $(2^{p-1})^2\equiv 1(\bmod p)$.

20. 利用费马定理和引理1.

21. $1+n+n^2+\cdots+n^{p-2}=(n^{p-1}-1)/(n-1)$.

22. 利用题21，且使$n=10$. 或者：你如果已经读过§15，就可注意到，由于$p\neq 2$或5，$1/p$可展开成一个循环小数：$1/p=0.\overline{d_1d_2\cdots d_k}$，因此，$(10^k-1)=p(d_1d_2\cdots d_k)$. 如$p\neq 3$，则有$p\mid(10^k-1)/9$；$p=3$时，另作说明也不难证得题中结论.

23. 记$a=c^n+kp$，则$a^{(p-1)/n}=(c^n+kp)^{(p-1)/n}\equiv c^{p-1}(\bmod p)$.

§ 7

13. $\sum_{d\mid n} d=\sum_{d\mid n} n/d$：一个和式中出现的各项与另一和式中各项完全相同，但次序颠倒了.

15. 利用题14和定理2.

18. 令$x=6+a$，$y=6+b$，则$ab=36$.

19. 令$x=N+a$，$y=N+b$，则$ab=N^2$. 共有$d(N^2)$个正值a和$d(N^2)$个负值a满足此式，其中有一个即为$-N$.

21. 取n为一素数p，且$p>3$.

22. 令$x+y=a$，$x-y=b$，则$ab=N$.

23. 对方程取模4，并考虑三种情况：x和y均为奇数；一奇一偶；两者均为偶数.

24．仿照课文推出．

§8

6．利用题5以及下列结论：对任何正整数N，有

$$\sum_{d|N} 1/d=\frac{1}{N}\sum_{d|N} N/d=\frac{1}{N}\sum_{d|N} d.$$

8．若p，n为亲和数，则$p+1=\sigma(p)=p+n$，这是不可能的．

9．若p^e，n为亲和数，则

$$\frac{p^{e+1}-1}{p-1}=\sigma(p^e)=p^e+n,$$

由此可得$n=(p^e-1)/(p-1)$．

10．(a) $1+p$的因子不外乎是1，2，3，…，$1+p$，而这些数的和为$(p^2+3p+2)/2$；

(b) 若p^2，n为亲和数，则由题9，$\sigma(1+p)=1+p+p^2$．

12．(f) 证明$s(pq)=2-(p-1)(q-1)$；

(g) 若n为合数，则$\sigma(n)>n+1$，故
$\sigma(2^k(2^{k+1}-1))=\sigma(2^k)\sigma(2^{k+1}-1)>(2^{k+1}-1)2^{k+1}$．

(h) 设$2^{k+1}-1=p$为一素数，则有$d=2^m$或$2^m p$，其中m满足$0\leqslant m<k$；证明$s(d)=-1$或$2^{k+1}-2^{m+1}$；

(i) 若$p\neq 2$，证明$s(2^k p)=(2^{k+1}-1)-p>0$．并考虑$p=2$的情况．

13．证明：$s(p^e)=(2p^e-p^{e+1}-1)/(p-1)$，并证$2p^e<p^{e+1}-1$．

14．考虑下列各种情况：$p=2$，$p=5$，$p\equiv 1, 3, 7, 9 \pmod{10}$．

15．证明：由于$2^6\equiv 1 \pmod 9$，每一素数$p(p\geqslant 5)$均满足$2^{p-1}\equiv 1$或$7 \pmod 9$．$p=3$时要分开考虑．

16．$2^{p-1}(2^p-1)=(1/2)(4^p-2^p)=(1/2)((3+1)^p-(3-1)^p)$；用二项式公式展开之．

17．若$P_2=p_2^{2e_2+1}$，则$Q_2=\sigma(P_2)$应为偶数．若$P_1=p^{4a+8}$，则$Q_1=1+p+p^2+\cdots+p^{4a+8}\equiv 0 \pmod 4$．

§9

8．此题貌似复杂，实际上不过是练习一下求和记号而已．

10．用a乘同余式两端，并应用定理1．

13．当且仅当$(t, m)=1$时，$(dt, dm)=d$．

14. 利用定理3的推论知：若m和n有一大于1的公因子，则

$$\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{p|m}\left(1-\frac{1}{p}\right) \text{ 比 } \prod_{p|mn}\left(1-\frac{1}{p}\right)$$

具有更多的小于1的因子.

16. 记$m=2^rM$, $n=2^sN$, 其中M和N均为奇数. 则$(M, N)=1$, 故$\phi(mn)=\phi(2^{r+s}MN)=2^{r+s-1}\phi(M)\phi(N)$. 再计算$\phi(m)\phi(n)$.

17. 记$m=p^rM$, $n=p^sN$, 其中$(p, M)=(p, N)=1$, 则$(M, N)=1$; 然后如题16那样利用ϕ是积性函数这一特性.

18. 记$n=2^kN$, 其中N为奇数，则$\phi(n)=\phi(2^k)\phi(N)=2^{k-1}\phi(N)$, 同时，$n/2=2^{k-1}N$.

19. 记$n=2^k3^jN$, 其中$(2, N)=(3, N)=1$, 然后如题18那样证下去.

20. 如题19那样写出n, 则有$\phi(n)=2^k3^{j-1}\phi(N)\leqslant 2^k3^{j-1}N$.

21. 证明：若$n-1$和$n+1$均为素数，且$n>4$, 则$6|n$. 然后应用题20的结果.

24. n的奇素因子个数不可能超过1.

25. 证明：n不可能具有2个以上不同的素因子，且对素数p, q和正整数a, b, 不可能成立$p^{a-1}(p-1)q^{b-1}(q-1)=14$.

27. 证明：若$1\leqslant m\leqslant n$, 且$(m, n)=1$, 则$(n-m, n)=1$. 因此，若$n>2$, 则小于n并与n互素的所有整数都可以成对地配起来，使每对的两数之和均为n.

§ 10

7. $\phi(10021)=9100=2^2\cdot5^2\cdot7\cdot13$.

9. (a) 应用引理2; (b) 2是37的一个原根.

11. 由于g是p的一个原根，故不可能有$g^{(p-1)/2}\equiv1 \pmod p$.

14. 用$a-1$乘此同余式左端.

15. (a) 若a为偶数，则$(h^a)^{(p-1)/2}\equiv1 \pmod p$;

    (b) 设k为p的任一原根. 由题15(a)知，有$g\equiv k^a$与$h\equiv k^b \pmod p$, 其中a和b为奇数. 因此，$a+b$为偶数，且$(gh)^{(p-1)/2}\equiv(k^{(a+b)/2})^{(p-1)}\equiv1 \pmod p$, 故$gh$的阶$\pmod p$不是$p-1$.

16. 因为 $a^2+a+1\equiv 0 \pmod p$，故 $(a+1)^6\equiv 21(a^2+a+1)+1\equiv 1 \pmod p$. 又，$(a+1)^3\equiv -1 \pmod p$，$(a+1)^2\equiv a \pmod p$.

17. 由定理 2，任一素因子的形式都为 $34k+1$，而且，最小的素因子必小于 $(131071)^{1/2}$，故也小于 362，要检验的素数就只有 103，137，239，307.

18. 将定理 2 的证明改造一下. a 的阶 $(\bmod q)$ 为 1，2，p 或 $2p$，证明 a 的阶不可能是 p. 再证，若 a 的阶为 2，则 $q\mid(a+1)$，且若 a 的阶为 $2p$，则 $q\equiv 1 \pmod{2p}$.

19. 由题 18，不等于 3 且能整除 $2^{19}+1$ 的素数的形式必为 $38k+1$. 由于 $((2^{19}+1)/3)^{1/2}<2^9$，要检验的素数就只有 191，229，419，457.

20. 若 $2\,\mathrm{ind}_g n=\mathrm{ind}_g(n+1)+\mathrm{ind}_g(n-1)$，则 $n^2\equiv(n+1)(n-1)\equiv n^2-1 \pmod p$，这不可能成立.

21. (a) 设 $n_1, n_2, \cdots, n_{\phi(m)}$ 为小于或等于 m 且与 m 互素的正整数，则 $\mathrm{ind}_g n_k (k=1, 2, \cdots, \phi(m))$ 这些数是 $0, 1, \cdots, \phi(m)-1$ 的一个排列. 因而有

$$n_1n_2\cdots n_{\phi(m)}\equiv g^{1+2+\cdots+\phi(m)-1}\equiv g^{\phi(m)(\phi(m)-1)/2}$$
$$\equiv g^{\phi(m)/2}\equiv -1 \pmod m.$$

22. (b) 若 $\mathrm{ind}_g h=a$，$\mathrm{ind}_h g=b$，则 $g\equiv h^b\equiv (g^a)^b \pmod m$.

23. 应用题 22 的结果.

§ 11

6. 它们恰好是 $1^2, 2^2, \cdots, 15^2$ 的最小剩余 $(\bmod 31)$.

7. (e) $22\equiv -1 \pmod{23}$.

12. 应用二次互反性定理.

17. 当且仅当 -1 是一个二次剩余 $(\bmod 7)$ 时，$7\mid(n^2+1)$.

18. $(1/p)=(ab/p)=(a/p)(b/p)$.

19. $159=3\cdot 53$，它不是素数. 考虑 $x^2\equiv 211 \pmod 3$ 和 $x^2\equiv 211 \pmod{53}$.

21. $(p/q)=((q+4a)/q)=(4a/q)=(a/q)$，$(q/p)=((p-4a)/p)=(-4a/p)=(-1/p)(a/p)$. 因此，$(p/q)(q/p)=(-1/p)(a/p)(a/q)$. 应用二次互反性定理：因 $p\equiv q \pmod 4$，故只有两种情况，即 $p\equiv q\equiv 1 \pmod 4$，或 $p\equiv q\equiv 3 \pmod 4$.

§ 12

1. 若$p>3$，则使$3k$的最小剩余$(\bmod p)$大于$(p-1)/2$的那些整数k正好是满足$(p-1)/6<k\leqslant(p-1)/3$的那些$k$．考虑下列几种情况：$p=12n+1$，5，7，11．
2. $p=4^n+1\equiv1(\bmod 4)$，故$(3/p)=(p/3)=(2/3)$．另一方法是：我们知，对所有正数n，有$4^n\equiv4(\bmod 12)$，再应用题1的结果．
3. 证明，若$p=2^q-1$，其中q为奇素数，则$p=2\cdot4^{(q-1)/2}-1\equiv-1(\bmod 4)$，故有$(3/p)=-(p/3)$．
4. (a) 2是一个二次剩余$(\bmod p)$，故由欧拉准则，$1=(2/p)\equiv2^{(p-1)/2}(\bmod p)$．
5. (a) 注意，我们总有$q\equiv1(\bmod 4)$；
   (b) 考虑两种情况：$p\equiv1(\bmod 4)$和$p\equiv3(\bmod 4)$．
7. $((p-a)/p)=(-a/p)$．
8. 各个剩余之和同余$(\bmod p)$于

$$1^2+2^2+\cdots+\left(\frac{p-1}{2}\right)^2.$$

9. (a) $(-3/p)=(-1/p)(3/p)$；应用题1的结果；
   (b) 证明，若$x^2+xr+r^2\equiv0(\bmod p)$，则$(x+s)^2\equiv-3s^2(\bmod p)$，其中$s$是$2s\equiv r(\bmod p)$的唯一解．
10. 设n'是$nn'\equiv1(\bmod p)$的唯一解，$n=1,2,\cdots,p-1$，则$n(1+n)\equiv n^2(1+n')(\bmod p)$，故$(n(n+1)/p)=((1+n')/p)$．证明，当$n$取遍1，2，…，$p-2$时，$1+n'$跑遍2，3，…，$p-1$．而我们要计算的和为$(2/p)+(3/p)+\cdots+((p-1)/p)$．但1，2，…，$p-1$各数中，有一半是剩余，另一半是非剩余，故有

$$(1/p)+(2/p)+\cdots+((p-1)/p)=0.$$

11. 利用§6题7的定理，取$k=(p+1)/2$．

§13

7. (b) 一种方法是利用几何级数的求和公式．
8. 考虑b分别与0，1，2，3，4同余$(\bmod 5)$这几种情况．
9. (b) $7^k\equiv1(\bmod 2)$，$k=0,1,2,\cdots$．
12. 用2为基来表示数时，检查一下有该数出现的表格有什么共同的特点．

基为九

13．欲证这样一个表示式的存在性，最好用归纳法．选取 r，使

$$\frac{3^r+1}{2}\leqslant n<\frac{3^{r+1}+1}{2},$$

则有 $(-3^r+1)/2\leqslant n-3^r<(3^r+1)/2$.

14．以 2 为基写出 100000.

16．应用题 13 的结果.

§ **14**

16．取 $2^{1/2}=(1.4142)_z$，并将它转换为以 10 为基的数.

17．$10^k\equiv 1(\text{mod }\varepsilon)$，$k=0,1,\cdots$.

19．一立方英尺的水重 62.5_z 普通磅，一普通加仑的水的体积为 231_z 立方英寸.

§ **15**

1．(e) $10^2\equiv -1(\text{mod }101)$.

5．设 $1/n=d_1/b+\cdots+d_t/b^t$，则 b^t/n 是一个整数。

6．证明存在一整数 t，使 b^t/n 为一整数.

8．仿照定理 4 的证明.

13．(e) $b(rb-(r-1))=r(b-1)^2+((r+1)b-r)$，$r=0,1,2,\cdots$.

14．若一个数展开后，既不是有限小数，又不是循环小数，则此数必定不是有理数．因此，用任何数(包括7在内)做基，0.101001000100001…总是无理数.

§ **16**

7．若 $n+(n+1)=m^2$，则 $n^2+m^2=(n+1)^2$.

8．若 $a^2+b^2=c^2$，且 $ab=2c$，则可证，$(a+b)^2=(c+2)^2-4=c(c+4)$，且 $(c,c+4)=1,2$，或 4；应用引理 2.

9．若 $m\equiv 0(\text{mod }5)$ 或 $n\equiv 0(\text{mod }5)$，则 $5|a$．若 $m\equiv \pm n(\text{mod }5)$，则 $5|b$．证明在余下的各种情况中，必有 $5|c$.

10．证明 $4|2mn(m^2-n^2)$ 和 $3|2mn(m^2-n^2)$.

11．将题 9 和题 10 合在一起考虑即可.

12．(a) 该四边形有两个直角.

13．设 $n=t(t-1)/2$，$m=t(t+1)/2$，计算 m^2-n^2.

15．若 $(a-d)^2+a^2=(a+d)^2$，则 $a(a-4d)=0$.

16. (b) 若 $a^2+b^2=(b+1)^2$，则 $a^2=2b+1$，因而 a 为奇数，可设 $a=2n+1$.

17. (b) 我们要找 $m_1n_1(m_1^2-n_1^2)=m_2n_2(m_2^2-n_2^2)$ 的非平凡解，这可不大容易.

18. 对模 2 考虑该方程.

19. 仅当 $4n^2+4n+1\equiv-1 \pmod k$ 时，有 $2n^2+2n+1\equiv0 \pmod k$.

21. 若 $9=(a/c)^2+(b/c)^2$，则 $a^2+b^2=9c^2$. 因此 $a^2+b^2\equiv0 \pmod 9$；证明这将意味着 $a=3r$, $b=3s$，因而有 $r^2+s^2=c^2$，此方程有无限多组解.

22. (a) 若 a 为偶数，求 m 和 n，使 $a=2mn$；若 a 为奇数，求 m 和 n，使 $a=m^2-n^2=(m+n)(m-n)$.

23. 若 $a^2+b^2=c^2$，且 $2(a+b+c)=ab$，证明 $b=4+8/(a-4)$，故只可能有 $a=5, 6, 8, 12$.

§ 17

3. 回忆一下费马定理.

4. 若 $p\nmid xyz$，则费马定理称：$x^{p-1}\equiv y^{p-1}\equiv z^{p-1}\equiv1 \pmod p$.

7. 证明 x, y, z 必定全为偶数.

10. 因不可能有 $x=y$，故可假定 $x>y$. 可证，$x^n<z^n$，且 $(x+1)^n\geqslant x^n+nx^{n-1}>x^n+y^n=z^n$，因此有 $x^n<z^n<(x+1)^n$，这是不可能的.

§ 18

3. 利用表 C 或表 B.

4. 因 $x^2\equiv0,1,2$ 或 $4 \pmod 7$，故仅当 $x\equiv y\equiv0 \pmod 7$ 时，有 $x^2+y^2\equiv0 \pmod 7$，但此时应有 $49\mid(x^2+y^2)$.

5. $x^2\equiv0, 1, 4$ 或 $7 \pmod 9$.

7. 考虑 n/m 的素数幂分解式.

12. $x^2\equiv0, 1$ 或 $4 \pmod 8$.

13. 假定 $4^e(8k+7)=x^2+y^2+z^2$. 反复应用题 11 的结果可得 $8k+7=x_1^2+y_1^2+z_1^2$，其中 x_1, y_1, z_1 均为整数. 再应用题 12 的结果.

15. 证明中可利用 $(r^2+ws^2)(x^2+wy^2)=(rx+wsy)^2+w(ry-sx)^2$.

§ 19

3. $5725841=11^2\cdot47321$.

6. 考虑三种情况: x, y, z, w 中, 至少有三数可被 3 整除; 恰有两数可被 3 整除; 至少有三数不能被 3 整除.

11. 若 $k_1, k_2, \cdots, k_r$ 全为奇数, 则 $k_1^2+k_2^2+\cdots+k_r^2\equiv r \pmod 8$.

12. 对模 4 考虑该式.

§ **20**

3. $x^2+2xy-2y^2=(x+y)^2-3y^2$.

5. 配成完全平方.

7. (a) 以 a, b, c 为三边的三角形面积为 $(s(s-a)(s-b)(s-c))^{1/2}$, 其中 $s=(a+b+c)/2$;

   (b) 若 $3a^2-3=b^2$, 则 $3|b$. 故 $b=3c$, 就有 $3a^2-3=9c^2$, 即 $a^2-3c^2=1$, 这是一个费马方程;

   (d) 对模 4 考虑 $3((2a+1)^2-4)=c^2$.

9. $x_1+y_1N^{1/2}>1$, $1=x_1^2-Ny_1^2=(x_1+y_1N^{1/2})(x_1-y_1N^{1/2})$.

13. 应用引理 2.

14. 若 $(x-1)^2+x^2+(x+1)^2=u^2+(u+1)^2$, 则 $(2u+1)^2=6x^2+3$, 故有 $2u+1=3y$, $3y^2-2x^2=1$. 用尝试法还可发现比 $x=11$, $y=9$ 更大的解.

15. 若 $1+n+n^2=m^2$, 就有 $4m^2-(2n+1)^2=3$, 将左端分解因子. 另一方法是利用 $n^2<n^2+n+1<(n+1)^2$.

§ **21**

2. 注意, 并不要求 $n\neq m$ 时有 $f(n)\neq f(m)$.

3. 一种方法是考虑 $n \pmod 7$ 和 $n \pmod{11}$ 的所有可能的情况.

5. -2 对哪些素数是二次剩余?

6. $n^2+2n+3=(n+1)^2+2$.

7. 考虑模为 2, 3 和 5 这几种情况.

8. 在 $n^2+n+41\equiv 0 \pmod p$ 中配完全平方.

9. 应用二项式公式.

11. 利用威尔逊定理.

13. 说明其条件即为: $n(n+1)|2n!$, 可考虑三种情况: $n+1$ 为偶数; $n+1$ 为奇平方数; $n+1$ 为奇合数. 证明, 在每种情况下, $n(n+1)$ 的因子都在 $2n!$ 的因子中出现.

14. 若$x+(x+1)+\cdots+(x+t)=p$，则$(t+1)(2x+t)=2p$，说明这将意味着$t=1$.

15. (d) 证明n在第n行中出现$\phi(n)$次. 这不很容易.

16. 利用对数.

§ 23

15. 证明$3|(p^2+2)$.

23. 对模3和模8考虑$ab(a+b)(a-b)$.

28. $(2/7)^2+(5/7)=(2/7)+(5/7)^2$.

33. (a) 若$n=a_0+a_1\cdot12+\cdots+a_k\cdot12^k$，则

$$m=a_k+a_{k-1}\cdot12+\cdots+a_0\cdot12^k,$$

计算$n-m \pmod{11}$.

34. (a) 若m为合数，则$p=2, 3, 5, 7$中必有一数整除m，从而也有$p|(210n+m)$.

35. (a) 若$3p+1=a^2$，则$3p=(a+1)(a-1)$;

(b) 若$3p+2=a^2$，则$a^2\equiv2 \pmod 3$.

36. 注意，假定$(a, b)=1$并不失去一般性. 将此方程右端配成完全平方，并对模4取同余式，看一看会得到什么.

37. 大家熟悉的"有理数根定理"称，若r/s为$a_nx^x+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$的一个根，则$r|a_0$，$s|a_n$. 故若$r/s$为$a^2+b^2=2(a+b)x+x^2$的一个根，则$r|(a^2+b^2)$，$s|1$. 注意，若$a+b\neq0$，且$x^2$是有理数，则

$$x=\frac{a^2+b^2-x^2}{2(a+b)}$$

也是有理数.

38. 以m, 4, 9为模考虑$n-1$.

39. 20413的素数幂分解式为$137\cdot149$.

40. (a) 若$n=ab$，则10^n-1是合数.

43. 考虑$2^{p-1}(2^p-1) \pmod{12}$.

46. 如其它方法用不上，可用归纳法.

48. 证明任一对孪生素数的第一个数必与5同余(mod 6).

51. 考虑所有的情况(mod 24).

52. $9^{10}\equiv1 \pmod{100}$.

53. 若$kp+b=m^2$，则$m^2\equiv b\equiv c^2(\mathrm{mod}\,p)$，故$m=\pm c(\mathrm{mod}\,p)$，也即对某整数$n$，有$m=\pm c+np$.

54. $3|(2^m+1)$.

55. $10^{3^{n+1}}-1=(10^{3^n}-1)(10^{2\cdot 3^n}+10^{3^n}+1)$.

57. $z^6-x^6=(z-x)(z^2+xz+x^2)(z^3+x^3)$. 证明右端各因子中至少有一个为奇数.

58. (a) 配完全平方.

59. (c) $ab\left(\frac{a+b}{2}\right)\left(\frac{a-b}{2}\right)=\left(\frac{c}{2}\right)^2$.

60. 若$n(n+1)/2=x^2$，则$(2n+1)^2=8x^2+1$. 若$y=2n+1$，则$y^2-8x^2=1$，这是一个生成元为$3+8^{1/2}$的费马方程，它有无限多组解.

61. 取x使$n-x^2=m$为正奇数，然后令$y=(m+1)/2$.

64. 证明，若x, y, z三数中，有一个、两个或三个为奇数，则此方程左端也为奇数.

65. 令$m=2pM_1$, $n=2qN_1$, $m+1=3qM_2$, $n+1=3pN_2$，其中p和q为不同的素数.

66. (a) 考虑此式的两端$(\mathrm{mod}\,3)$.

    (b) $n^2+(n+1)^2+\cdots+(n+k)^2=(k+1)n^2+k(k+1)n+\sum_{r=1}^{k}r^2$.

67. 在$n!$的各因子中，每出现一个因子5，必另有两个偶数因子出现.

68. $n+(n+1)+\cdots+(n+d)=(2n+d)(d+1)/2$；若它是2的某次幂，证明$d$既不是奇数又不是偶数.

70. 考虑此数$(\mathrm{mod}\,10)$.

71. 设这些整数为$a-4b$, $a-3b$, $\cdots$, $a+4b$，则它们的平方和为$9a^2+60b^2$.

73. $\phi(n)\leqslant n\left(1-\frac{1}{p}\right)$，其中$p$是整除$n$的最小素数，且$p\leqslant n^{1/2}$.

76. 若p为素数，则由威尔逊定理知，

$$\begin{aligned}4((p-1)!+1)&\equiv -p(p+1)p((p-1)!+1)\\&\equiv -p((p+1)!+2)(\mathrm{mod}\,(p+2)),\end{aligned}$$

当且仅当$p+2$为素数时，有$(p+1)!\equiv -1(\mathrm{mod}\,(p+2))$.

81. 若$p>12$，则$p-9$为偶合数.

82. 若$p^{a-1}(p-1)=q^{b-1}(q-1)$，且$a>1$，则$p|(q-1)$，这与$p>q$矛盾.

85. (a) 令$y=x+d$, $z=x+2d$，则$(d+x)(3d-2x)=0$;

(b) 若$y=x+d$, $z=x+2d$，则$(d+x)(3d-(k+1)x)=0$.

87. $a_1, a_2, \cdots, a_k$ 的调和平均数 m 由下式给出:

$$\frac{1}{m}=\frac{1}{k}\left(\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_k}\right).$$

因此，对于一个偶完全数n的因子，有

$$\frac{1}{m}=\frac{1}{d(n)}\sum_{d|n}\frac{1}{d}=\frac{1}{nd(n)}\sum_{d|n}\frac{n}{d}=\frac{2}{d(n)}.$$

88. (b) 若$n\equiv1 \pmod 3$，则$3|p^r$，故$p=3$.但$n\equiv1,4$或$7 \pmod 9$，故$n^2+n+1\equiv3 \pmod 9$. 因而，$r=n=1$;

(c) 若$r=2k$，则$(2n+1)^2-(2p^k)^2=3$. 将左端分解因子;

(d) 假设$p\neq3$，且$p\equiv2 \pmod 3$. 因r为奇数，$p^r\equiv2 \pmod 3$. 另外，$n^2+n+1\equiv1 \pmod 3$.

89. 若$f(r/s)=0$，则$r|a_n$, $s|a_0$. 因此，r和s均为奇数，但这意味着$0=s^nf(r/s)$是一些偶数与奇数个奇数相加所得的和，这是不可能的.

90. 求r和s，使$(p-1)r+1=sn$，然后令$x=n^s$.

91. (a) 若$x^n\equiv a$，则$1\equiv x^{p-1}\equiv(x^n)^{(p-1)/n}\equiv a^{(p-1)/n} \pmod p$.

92. 一种有效的方法是归纳法，并利用下列恒等式:

$$2^{3^{k+1}}+1=(2^{3^k}+1)(2^{2\cdot 3^k}-2^{3^k}+1).$$

93. (a) 若不然，则$2n^2+2n+(1-3m^2)=0$，故$2n=-1\pm(6m^2-1)^{1/2}$，因此对某r，有$6m^2-1=r^2$，但$r^2\equiv-1 \pmod 6$不可能成立.

94. 设$m=p_1p_2\cdots p_k$，其中$p_1<p_2<\cdots<p_k$，则由$p_2|m$，可得$(p_2-1)|m$，故$p_2-1=p_1$，因此$p_1=2$, $p_2=3$.另外，由$p_3|m$，得$(p_3-1)|m$，故$(p_3-1)|p_1p_2$，从而$p_3=7$. 类似地，由$(p_4-1)|42$，得$p_4=43$.最后，应有$(p_5-1)|2\cdot3\cdot7\cdot43$，但这样的素数不存在.

96. 乘积中各素数整除$(2n)!$，但不能整除$n!$.

98. $n^{2^m}\equiv n^{p-1}\equiv1 \pmod p$，且$-1\equiv(n/p)\equiv n^{(p-1)/2}\equiv n^{2^{m-1}} \pmod p$，故$n$的阶为$2^m \pmod p$.

103. (a) $x^2=10^nrs+x$.

104. 假定n为素数. 由威尔逊定理，对某k，有$1+(n-1)!=kn$，因而，

对所有 j，有 $\alpha^{j(1+(n-1)!)}=\alpha^{jkn}=(\alpha^n)^{jk}=1$. 若 n 为大于 4 的合数，则对某 k，有 $1+(n-1)!=1+kn$，故 $\alpha^{j(1+(n-1)!)}=\alpha^j$，其和式为几何级数，它加起来等于零. 当 $n=4$ 时，此和也是零.

105．应用费马定理:从任一项开始，都有一个公比为 2^{p-1} 的几何级数.

附录一

4．$1^3+2^3+\cdots+n^3=(n(n+1)/2)^2$.

8．$(n-1)n(n+1)(n+2)=(n^2+n-1)^2-1$.

10．$(n+1)(n+2)(n+3)=n(n+1)(n+2)+3(n+1)(n+2)$，而 $(n+1)(n+2)$ 是偶数.

附录二

19．计算一下每一素因子在两端各出现多少次.

20．应用题 15 的结果:

$$\frac{1}{n}\sum_{d|n}d=\sum_{d|n}\frac{1}{d},\quad \frac{1}{n^2}\sum_{d|n}d^2=\sum_{d|n}\frac{1}{d^2}.$$

23．在该式两端同乘 $n_1n_2\cdots n_k$.

习 题 答 案

§ **1**

1. (a) 1; (b) 1; (c) 592; (d) 73.

5. 例如，$2\nmid(-4)$.

6. (b) 1 或 2. (c) k 的一个正因子.

9. (a) $x=-40,\ y=79$; (b) $x=37,\ y=-73$;
   (c) $x=2,\ y=-1$; (d) $x=-10,\ y=1$.
   各方程都还有其它的解.

10. (b) 对; (c) 对.

11. (b) $x=5+19t,\ y=-6-23t$，其中 t 为整数. 这给出了方程的所有解;
    (c) $x=1+19t,\ y=-1-23t$，其中 t 为整数. 这给出了方程的所有解.

17. 例如，$4\nmid 6$，但 $(4,6)=2$.

20. (b) $m=2,\ 6,\ 10,\ 14,\ \cdots$.

§ **2**

1. (a) $3\cdot37$; (b) $2\cdot617$; (c) $5\cdot7\cdot67$; (d) $2^7\cdot3^3$;
   (e) 素数; (f) $3\cdot7\cdot11\cdot13\cdot37$; (g) $3^3\cdot7\cdot11\cdot13\cdot37\cdot101\cdot9901$.

2. 例如，$6\mid4\cdot9$，但 $6\nmid4$，$6\nmid9$.

3. $511=7\cdot73$.

4. (a) 使这个说法不成立的第一个数为 $n=20$; $119=7\cdot17$, $121=11^2$. $n=24,\ 31,\ 36$ 时，这个结论也不成立.

5. 不.

7. 当且仅当 n 的素数幂分解式中每一幂指数均能被 k 整除时，n 是一个 k 次乘幂.

8. 不能.

9. 对所有 $n>0$, 有 $n^2<n(n+1)<(n+1)^2$, 由此可得题中结论.

10. (b) 没有,因为无论数字 a 和 b 是什么,总有

$$78 \leqslant \frac{25ab}{32} < 82.$$

11. 只有 $p=19$.

12. (a) 7; (c) 若 $n=1001!+1$, 则 $n+1, n+2, \cdots, n+1000$ 均为合数.

14. 不成立: $2^{11}-1=2047=23\cdot89$ 是合数(利用表 A 可知), 但 11 却不是合数.

16. 不成立: $3|60$, $5|60$, 且 3 和 5 均大于 $60^{1/4}=2.78\cdots$, 但 $60/3\cdot5=4$ 不是素数. 要是 p 和 q 是 n 的最小素因子的话, 这一命题就成立了.

17. (a) 60, $2p^2q$.

19. (b) $b+a$ 和 $b-a$; (c) $1189=29\cdot41$; (d) $9379=83\cdot113$.

§ 3

1. (a) $x=1+t$, $y=1-t$; (b) $x=1+t$, $y=-2t$;
   (c) $x=-1+16t$, $y=2-15t$; (d) 无解.
   在(a), (b), (c)中, t 是任意整数. 还可用别的方法写出解来, 例如,在(c)中, $x=-17+16s$, $y=17-15s$, s 为整数,这给出了与上述完全相同的解的集合.

2. (a) $x, y=1, 1$; (b) 无解;
   (c) $x, y=1, 3$ 或 $6, 1$; (d) $x, y=3, 2$.

3. (a) $x=-4-5t$, $y=-5-2t$, $t=0, 1, 2, \cdots$; (b) 无解.

4. $x, y, z=22, 8, 1; 23, 6, 2; 24, 4, 3; 25, 2, 4$.

5. 21 条蚯蚓.

6. 他买了九个苹果和三个桔子,苹果每个 9 分,桔子每个 6 分.

7. 5 头牛.

8. 有四种方法. 二角五分的钞票分别是 14 张, 15 张, 16 张, 17 张.

9. 二年级学生 8 名,三年级学生 15 名,四年级学生 3 名.

10. A 有 10 元, B 有 75 元, C 有 15 元.

11. 安娜是 5 岁,玛丽是 12 岁.

13. 解的一种表达式为: $x=-1-9m+8n,\ y=1+9m-7n,\ z=-m$, 其中 m 和 n 为任意整数. 解的另一表达式为: $x=7+63m+8n$, $y=-6-54m-7n,\ z=-m$.
14. 25.51 元.
15. 降价后价格是每个蛋 3 分, 每人至少卖得 1.20 元.

§ 4

2. 一个反例: $2^2\equiv 3^2 \pmod 5$, 但 $2\not\equiv 3 \pmod 5$.
3. 不成立. 一个反例: $1\equiv 4 \pmod 3$, 但 $1^2\not\equiv 4^2 \pmod 9$.
4. 3.
7. 1, 7, 11, 13, 17, 19, 23, 29.
8. 6.
16. (c) 将一个整数的各位数字从右向左交替地配以正号和负号, 然后将它们相加, 所得之数若能被 11 整除, 则此整数就能被 11 整除. 这可用另一方式叙述如下: 设 n 的序号为偶数的各位数字之和为 a, 其余各位数字之和为 b, 若 $11\mid(a-b)$, 则 $11\mid n$.
17. 甲.
19. 1996 年, 2024 年, 2052 年, 2080 年.
20. 位数是偶数的任一回文数都可被 11 整除.
22. 任何 $n\equiv 15 \pmod{30}$ 都满足这三个同余式.
24. 因 $x\equiv 1 \pmod m$, 故

$$x^{m-1}+x^{m-2}+\cdots+1\equiv 1+1+\cdots+1\equiv 0 \pmod m.$$

25. $118050660=2^2\cdot 3^2\cdot 5\cdot 7\cdot 13\cdot 7207$.

§ 5

1. (a) 9; (b) 6; (c) 2, 8, 14; (d) 6, 15; (e) 6041.
2. 例如, $15x\equiv 14$, $13x\equiv 14$, $12x\equiv 14$, $20x\equiv 0 \pmod{20}$ 分别为无解、有 1 个解、4 个解和 20 个解.
3. 解数可能为 0, 1, 2, 4, 5, 10, 20.
4. (a) $x\equiv 1 \pmod 6$; (b) $x\equiv 13 \pmod{42}$; (c) $x\equiv 348 \pmod{385}$; (d) $x\equiv 3 \pmod{385}$; (e) $x\equiv 605 \pmod{1066}$.
5. $x\equiv 534 \pmod{2401}$.
6. 17 人或 157 人, 等等.

7. 213.

8. $2^{15}3^{10}5^6=30233088000000$.

9. 301 或任何与 301 同余(mod 420)的数.

10. (a) 2223 或任何与 2223 同余(mod 3600)的数; (b) 不能.

12. (a) $x=3,\ y=0$; (b) $x=5,\ y=5$.

13. 28, 21, 18; 63, 42, 33; 98, 63, 48.

15. 62.

16. 对所有 $i,\ j$, 有 $(m_i,\ m_j)\mid(a_i-a_j)$. 可证此条件也是该同余式组有解的充分条件.

17. $(a,\ b)$.

§ **6**

1. 6.

2. 1.

3. 3.

4. 43.

7. $(p-k)!\,(k-1)!\equiv(-1)^k \pmod p$, $k=0,\ 1,\ \cdots,\ p$.

8. (a) 2, 0, 0, 0, 0;

   (b) 若 $n>4$ 为合数,则 $(n-1)!\equiv 0 \pmod n$;

10. (b) 例如, $p=5,\ r=3$, 或者, $p=7,\ r=3$ 或 5.

20. 1 或 -1.

21. 所有满足 $n\not\equiv 0$ 或 $1 \pmod p$ 的数 n.

§ **7**

1. (a) 8; (b) 24; (c) 48.

2. (a) 96; (b) 1334; (c) 14880.

3. (a) 4; (b) 24; (c) 4.

4. (a) $74\cdot 138=10212$; (b) $12\cdot 9092=109104$;

   (c) $15\cdot 13\cdot 140=27300$.

8. 例如, $d(n)-n$ 不是积性函数.

9. 24, 48.

10. 是: $d(2^{k-1})=k$.

11. $2^4\cdot 3^2\cdot 5\cdot 7=5040$. 还有 $2^4\cdot 3^2\cdot 5\cdot 11=7920$, $2^4\cdot 3^2\cdot 5\cdot 13=9360$.

12. 对任何素数 p，都有 $d(p^{59})=60$.

14. k 为偶数时.

15. 形为 $2^e p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$ 的一切 n.

18. 16 组解是: $(x, y)=(2, -3)$, $(3, -6)$, $(4, -12)$, $(5, -30)$, $(7, 42)$, $(8, 24)$, $(9, 18)$, $(10, 15)$, 以及将它们中两个数次序调换后所得的 8 组解. 第 17 组解为 $(x, y)=(12, 12)$.

19. $2d(N^2)-1$.

22. $2d(N)$.

24. 若 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, 则 $\sigma_2(n)=(1+p_1^2+p_1^4+\cdots+p_1^{2e_1})$
$$(1+p_2^2+\cdots+p_2^{2e_2})\cdots(1+p_k^2+\cdots+p_k^{2e_k}).$$

25. 若 $n=\prod_{p|n} p^{e_p}$, 则 $\sigma_k(n)=\prod_{p|n}\dfrac{p^{(e_p+1)k}-1}{p^k-1}$.

§ 8

3. $2^{p-1}(2^p-1)=n(n+1)/2$, 其中 $n=2^p-1$.

4. 可以. $2^{p-1}(2^p-1)=1+2+\cdots+(2^p-1)$.

4. (b) 6 是完全数; 12, 18, 20 为过剩数; 其余各数为亏缺数;

(c) $s(945)=30$;

(d)

n	3	4	5	6	7	8	9	10
$n(n+1)$	12	20	30	42	56	72	90	110
$\sigma(n(n+1))$	28	42	72	96	120	195	234	216
$s(n(n+1))$	4	2	12	10	8	51	54	-4.

§ 9

1. 12, 96, 960.

2. 9792, 90900.

4. 1, 5, 7, 11, 13, 17.

5. 没有数满足 $\phi(n)=2n$, 因为对所有 n, 有 $\phi(n)\leqslant n$.

7. 所有小于 n 且与 n 互素的正整数之和为 $n\phi(n)/2$.

11. (a) $p-2$;

(b) p^2-2p;

(c) 设 $\psi(n)$ 是序列 $1\cdot 2, 2\cdot 3, \cdots, n(n+1)$ 中与 n 互素的元素的个数. 若 $n=p^k$, p 为奇素数, 则 $\psi(n)=p^{k-1}(p-2)$. ψ 是积性函数, 因此对任何正整数 n 均可求出 $\psi(n)$.

12. 所有解为: 17, 32, 34, 40, 48, 60.

15. (a) 1, 1, 2, 1, 2, 2, 2; (b) $k-1$; (c) k; (d) $j+k-1$.

17. $\phi(mn)=(p/(p-1))\phi(m)\phi(n)$.

23. (a) 0, −13, 0, −15, 0; (b) $-p$; (c) 0; (d) $-p^k$;

(e) $\sum_{d\mid n}(-1)^{n/d}\phi(d)=\begin{cases}-n, & \text{当 } n \text{ 为奇数时,}\\ 0, & \text{当 } n \text{ 为偶数时.}\end{cases}$

24. $n=1, 2, 4, p^k$ 或 $2p^k$, 其中 $p\equiv 3 \pmod 4$, k 为正整数.

26. $k<50$ 时, 满足要求的 $2k$ 有: 14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98.

28. (a) 没有: 至少有一只角, 它的两个坐标均为偶数;

(b) 最靠近原点的这种方格的四只角为 (14, 20), (14, 21), (15, 20), (15, 21);

(c) $2\phi(p+1)-3$.

§ 10

1. (a) 199, 202; (b) 10198, 10201, 10202.

2. 4, 2, 4, 4, 2, 4, 2. (故 15 无原根.)

3. (a)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\text{ind}_2 n$	0	1	5	2	22	6	12	3	10	23	25	7	18	13
n	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\text{ind}_2 n$	27	4	21	11	9	24	17	26	20	8	16	19	15	14;

(b) 26;

(c) 11.

4. (a) 1; (b) 0; (c) 3.

5. (c) 不是.

6. 不存在.

7. 乙是正确的.

9. (b) 37 的原根是 2^k 的最小剩余(mod 37) (其中 $(k, 36)=1$), 也即为下列各数的最小剩余: $2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}, 2^{19}, 2^{23}, 2^{25}, 2^{29}, 2^{31}, 2^{35}$. 因此, 37 的原根为: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35;

10. (a) 2, 6, 7, 8; (b) 分别为 7, 3, 1, 9.

12. (b) $p-4$.

13. 6, 26.

21. (b) 例如，$m=8$.

22. (a) 若 g 和 h 是 m 的两个原根，则 $(\mathrm{ind}_g h)(\mathrm{ind}_h g)\equiv 1(\bmod \phi(m))$.

23. $g=h$ 等.

§ 11

1. (a); (b); (c); (d)均有解.
2. (a) 22, 31; (b) 2, 5; (c) 13, 18; (d) 25, 9948.
3. (a) 无解; (b) 0, 4; (c) 2.
4. (a) 四解: 1, 7, 9, 15. (b) 与定理1并不矛盾: 16并不是奇素数.
5. (a) 3, 6; (b) 4, 5.
6. 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28.
7. (a) 1; (b) 1; (c) 1; (d) -1; (e) -1; (f) -1.
8. 3, 11, 17.
9. (a) -1; (b) -1; (c) -1; (d) 1.
10. (a) 1; (b) 1.

13. 有解: 21, 76; 有解: 16, 37.

15. 是一个剩余.

16. 是.

17. $(-1/7)=-1$; 甲失败了.

19. 有解. 23, 76, 83, 136 即为所有解.

20. $(r/p)=1$.

§ 12

1. $(3/p)\begin{cases}1, & \text{当 } p\equiv 1 \text{ 或 } 11(\bmod 12)\text{时};\\ -1, & \text{当 } p\equiv 5 \text{ 或 } 7(\bmod 12)\text{时}.\end{cases}$

4. (b) 167.

6. (a) $p=2$ 和满足 $(-1/p)=1$ 的奇数 p，也即: $p=2$ 和 $p\equiv 1(\bmod 4)$;
   (b) 所有奇素数均满足 $p\mid(p^2+p)$;
   (c) 与1同余(mod 4)的奇素数.

7. (b) p 和 $p-a$ 同为剩余或同为非剩余.

§ 13

1. (a) 10111010100_2; (b) 2001021_3; (c) 4231_7; (d) 2037_9; (e) 1137_{11}.
2. (a) 421; (b) 709; (c) 1107; (d) 2305.
3. (a) 102; (b) 153; (c) 7.
4.

+	1	2	3	4	5	6	10
5	6	10	11	12	13	14	15
6	10	11	12	13	14	15	16
10	11	12	13	14	15	16	20 .

5.

·	2	3	4	5	6	10
5	13	21	26	34	42	50
6	15	24	33	42	51	60 .

6. (下列答数均以 7 为基)(a) 105; (b) 1445; (c) 534; (d) 54421.
7. (a) 19/49; (b) 1/2; (c) 13/16.
9. (c) 满足 $b\equiv1 \pmod 2$ 的任何数 b.
10. (b) $121_b=(b+1)^2$; (c) $(b+3)^2$.
12. 例如, 19=16+2+1, 它出现在表 16、表 2 和表 1 中.
14. 分成六份, 分别是 32 元, 128 元, 512 元, 1024 元, 32768 元, 65536 元.
15. 他赢了第 1, 2, 3, 4, 8 局.
16. 1 磅、3 磅、9 磅、27 磅、81 磅,用这五个砝码就可称出重量不超过 121 磅的任何物体的重量.

§ 14

1. $32=2\cdot17$, $33=3\cdot11$, $34=2^3\cdot5$, $36=2\cdot3\cdot7$, $38=2^2\cdot\varepsilon$, $39=3^2\cdot5$, $3\chi=2\cdot1\varepsilon$, $40=2^4\cdot3$, 而 31, 35, 37, 3ε 都是素数.
2. (a) $8\chi67$; (b) $-27\chi5$; (c) $15\varepsilon43126$; (d) 0.658; 余数是 $19\chi0$.
3. (a) 2454; (b) 156000; (c) $1/3^3=1/23\doteq0.054$.
6. $4\varepsilon.\varepsilon6=(59.95833\cdots)_\chi$.

χ. 次数大于 1 时 x 的各个乘幂的末位数字如下:

x　　0 1 2　3 4　5 6 7　8　9 χ ε

x^n之末位数 0 1 4, 8 3, 9 4 1, 5 0 1, 7 4, 8 9 4 ε.

ε. 除去素数 2 和 3 以外，其它素数的末位数只可能是 1, 5, 7, ε.

12. (a) 错，对，错.

13. 不能: $55=5\cdot 11$.

14. $24/9$, $9/\varepsilon\varepsilon$.

15. $3.\overline{86\chi351}$, $0.\overline{0\varepsilon}$.

16. $2^{1/2}=1.4\varepsilon792\cdots$; 1.5 是一个很精确的近似值.

18. 设一个整数为 $d_k d_{k-1}\cdots d_1 d_0$, 若 $(d_2d_1d_0)-(d_5d_4d_3)+(d_8d_7d_6)-\cdots$ 能被 7, 11 或 17 整除，则原整数就能被 7, 11 或 17 整除.

19. 本题下面答案中各数均以 χ 为基. 1 英里(十二进制) $=1728/1760=0.98\cdots$(普通)英里; 1 立方码等于 1728 品脱 (十二进制) 或 1616 (普通)品脱; 1 品脱(十二进制) $=0.93\cdots$(普通)品脱; 1 立方码可装水 1728 磅(十二进制), 它大约为 $27(62.5)=1687.5$ (普通)磅; 1 磅(十二进制) $=0.98\cdots$(普通)磅.

1χ. (a) 265 天，闰年有 266 天;

(b) 只有 260, 261, ⋯, 269;

(c) 没有: 若此数为 $abcd$, 则以 χ 为基时，我们有

$$1728a+144b+12c+d=1000(a+1)+100b+10c+d,$$

即
$$264a+22b+c=500,$$

对于 $0\leqslant a\leqslant 9$, $0\leqslant b\leqslant 9$, $0\leqslant c\leqslant 9$, 上述方程无解.

§ **15**

1. (a) 2;　(b) 3;　(c) 1;　(d) 3;　(e) 4;　(f) 6.
2. (a) 2;　(b) 3.
3. 乙说得对. $31415=5\cdot 6283$, 故 $1/31415$ 的循环节长至多是 6282. 事实上, $6283=61\cdot 103$, 而 $10^{3060}\equiv 1 \pmod{6283}$.

7. $1/16$, $1/18$, $1/24$.

9. (a) 2;　(b) 4;　(c) 3;　(d) 6;　(e) 10.

10. (a) $0.\overline{01}$;　(b) $0.\overline{0011}$;　(c) $0.\overline{000111}$.

11. (a) 6;　(b) 1;　(c) 16.

12. (a) $0.\overline{0\varepsilon}$;　(b) $0.0\overline{\chi35186}$.

13. (a) $0.\overline{012345679}$; (b) $0.\overline{0123457}$; (c) $0.\overline{012345}$.

(d) 以 b 为基，有 $1/(b-1)^2=0.\overline{012\cdots(b-4)(b-3)(b-1)}$.

§ 16

1. 还有 11 个:

a	8	12	16	20	24	28	32	36	24	36	16
b	6	9	12	15	18	21	24	27	10	15	30
c	10	15	20	25	30	35	40	45	26	39	34

2. 取 $m=10$, $n=3$, 即可找出一个来.

4. (b) $m=9$, $n=4$.

5. 能.

9. 是.

11. 由题 9 和题 10 证得.

12. (a) 234;

(b) 另一个四边形的四边为 33, 56, 63, 16, 一条对角线为 65;

(c) 能: 将两个斜边相等的毕达哥拉斯三角形沿斜边粘结在一起即构成这样的四边形. 为了说明这种四边形有无穷多个, 可取 c 为能被 5 整除的数. 要做到这一点, 可取 $m\equiv1(\bmod 5)$, $n\equiv2(\bmod 5)$. 例如, $c=5k$, 而设 a 和 b 是构成基本解的其它两边长. 由于 $3k$, $4k$, $5k$ 构成了一个毕达哥拉斯三角形, 其斜边为 $5k$. 故边长为 a, b, $3k$, $4k$ 的四边形的各边长都是整数, 且面积为 $\frac{1}{2}ab+6k^2$.

14. 由 $(n-1)^2+n^2=(n+1)^2$, 即得 $n^2=4n$. 因 $n>0$, 故 $n=4$.

16. (a) $(2n+1)^2+(2n(n+1))^2=(2n(n+1)+1)^2$, $n=0, 1, \cdots$.

17. (a) (20, 21, 29) 和 (12, 35, 36), 它们的面积为 210;

(b) 分别由 35, 11 和 33, 23 生成的两个三角形面积相同;

(c) 设两个三角形的各边分别为 a, b, c 和 a_1, b_1, c, 则 $a^2+b^2=a_1^2+b_1^2$, $ab=a_1b_1$, 从而得 $a=a_1$, $b=b_1$.

21. $9=(12/5)^2+(9/5)^2=(36/13)^2+(15/13)^2=(24/17)^2+(45/17)^2=\cdots$.

22. (b) 例如, $13^2+84^2=85^2$, $14^2+48^2=50^2$.

23. 这种三角形只有两个：5, 12, 13 和 6, 8, 10.

24. (b) 下一个这样的关系式为 $696^2+697^2=985^2$

§ **17**

5. 没有.

6. k 为偶数.

8. 是的. n^2 与 $n+1$ 互素.

9. $x=y=z=2$ 是一组解. 在题 8 中，取 $a=b=1$, $r=4$, $s=13$ 可得另一组解：$x=y=2^{16}$, $z=2^{13}$.

11. 设 $x=(ac)^{rn}$, $y=(bc)^{rn}$, $z=c^s$, 其中 $c=a^{rn^2}+b^{rn^2}$, $rn^2+1=(n-1)s$.

12. 如题 11 那样求解，不过这时有 $rn^2+1=ms$. 当 $(n^2, m)=1$ 时，此式有解.

§ **18**

1. $153=12^2+3^2$.

2. $1970=41^2+17^2$.

3. $10045=98^2+21^2=91^2+42^2$; $10048=88^2+48^2$;
   $10049=100^2+7^2=95^2+32^2$.

6. 不正确.

10. 102, 103, 111, 119, 124, 127, 135, 143.

14. 正确的.

15. 这一推广是错误的：$(-5/3)=1$，但 $x^2+5y^2=3$ 不可能成立.

16. 若 $n=x(x+1)/2+y(y+1)/2$，则 $4n+1=(x+y+1)^2+(x-y)^2$.

17. 若 $n=(a/c)^2+(b/c)^2$，则 $c^2n=a^2+b^2$. 又，当且仅当 n 可表为两平方数之和时，c^2n 可表为两平方数之和，故本题答案是："与定理 1 中说明的整数相同".

§ **19**

1. 记 $n=x^2+y^2+z^2+w^2$，我们有

n	(x, y, z, w)
2	(1, 1, 0, 0)
3	(1, 1, 1, 0)
5	(2, 1, 0, 0)

7 (2, 1, 1, 1)

11 (3, 1, 1, 0)

13 (3, 2, 0, 0) 或 (2, 2, 2, 1)

17 (4, 1, 0, 0) 或 (3, 2, 2, 0)

19 (4, 1, 1, 1) 或 (3, 3, 1, 0)

23 (3, 3, 2, 1).

2. (a) $121 = 11^2+0^2+0^2+0^2 = 10^2+4^2+2^2+1^2 = \cdots$
$= 7^2+6^2+6^2+0^2$;

(b) $391 = 19^2+5^2+2^2+1^2$;

(c) $47321 = 217^2+14^2+6^2+0^2$.

(a), (b), (c)都还有不少其它的表示式.

3. 其中一个表示式为: $2387^2+154^2+66^2+0^2$.

4. $112^2+63^2+35^2+21^2$.

7. 11, 14, 15.

9. $170^2+68^2+4^2+1^2$.

§ 20

1. (a) $5+2\cdot 6^{1/2}$; (b) $8+3\cdot 7^{1/2}$;

(c) $3+8^{1/2}$; (d) $19+6\cdot 10^{1/2}$;

(e) $10+3\cdot 11^{1/2}$; (f) $7+2\cdot 12^{1/2}$.

2. 两组最小的非平凡正数解为

(a) 5, 2 和 49, 20; (b) 3, 1 和 17, 6;

(c) 7, 2 和 97, 28; (d) 15, 4 和 449, 120;

(e) 8, 1 和 127, 16; (f) 10, 1 和 199, 20.

3. 三组最小的非平凡正数解为: $x, y = 1, 1; 3, 4; 11, 15$.

4. $x_k, y_k (k=1, 2, \cdots)$是一组解, 应满足:

$$(x_k+y_k)+y_k\cdot 3^{1/2} = (2+3^{1/2})^k.$$

5. (c) 该方程变成 $x+ay=1$ 或 $x+ay=-1$, 两者均有无限多组解.

6. (a) 生成该三角形的两数 m_k 和 n_k 由下式给出:

$$m_k-n_k+n_k\cdot 2^{1/2} = (3+2\cdot 2^{1/2})^k, k \text{ 为任意整数};$$

(b) (3, 4, 5), (696, 697, 993).

7. (b) (3, 4, 5), 面积为 6; (13, 14, 15), 面积为 84; (51, 52, 53),

面积为 1170.

10. x_k/y_k 愈来愈靠近 $N^{1/2}$.

11. 当 $k=1, 2, 3, 4$ 时, $x_k/y_k=3/2, 17/12, 99/70, 577/408$. x_k/y_k 与 $2^{1/2}$ 之差分别约为 0.09, 0.002, 0.00007, 0.000002.

14. 接下去的一个例子是 $108^2+109^2+110^2=133^2+134^2$.

17. $x_5=6(577)-99=3363$, $y_5=6(408)-70=2378$, 故有 $3363/2378=1.41421360\cdots$.

§ 21

1. $f(x)=(x^2+x+4)/2$.

2. 例如, $y=3$.

3. $n^2+21n+1\equiv n^2+1 \pmod 7$, -1 不是一个二次剩余 $(\bmod 7)$. $n^2+21n+1\equiv(n+5)^2-2 \pmod{11}$, 2 不是一个二次剩余 $(\bmod 11)$.

5. $p\equiv 1$ 或 $3 \pmod 8$; 还有 $p=2$.

6. $p\equiv 1$ 或 $3 \pmod 8$; 还有 $p=2$.

7. 11, 17, 41, 47, 71, 77.

16. 约为 10^{38}.

§ 22

2. $\frac{1}{6}\log\log x\leqslant\sum_{p<x}\frac{1}{p}\leqslant\frac{10}{3}\log\log x$.

3. $\frac{1}{3}\log N\leqslant\sum_{n<N}(\log p_n)/p_n\leqslant\frac{10}{3}(\log N+1)$.

5. (b) r_p.

§ 23

2. 40 张六分邮票, 10 张五分邮票, 21 张一角邮票.

3. $2^{27}-1=7\cdot 73\cdot 262657$.

5. (a) 0, 1, 4, 7; (b) 不是, 它与 2 同余 $(\bmod 9)$.

6. (b) 若 $a=2$, $b=3$, $p=5$, 那么 $(a+b)'$ 甚至都不存在, 更谈不上它与 $a'+b'$ 同余 $(\bmod p)$ 了.

7. 115, 117, 119, 121, 123, 125.

9. 帕斯卡已经发现了下列恒等式:

$$(n+1)^3-n^3-1=6\left(\frac{n(n+1)}{2}\right).$$

11．这些式子左端第一个数都是一些三角形数的平方．其结果可写为
$(2n^2+n)^2+\cdots+(2n^2+2n)^2=(2n^2+2n+1)^2+\cdots+(2n^2+3n)^2$.

12．(a) 9个； (b) 90个； (c) 若$k=2n$，则有$9\cdot 10^{n-1}$个；若$k=2n-1$，则有$9\cdot 10^{n-1}$个．

13．(c) 不成立．可举出无数个反例来说明这一点．

14．k应满足$(k, k(k+1)/2)=1$，也即$k=1$，或2.

16．1个男人，5个妇女，14个小孩．

17．(0)性质(l)，(m)，(n)对普通整除性不成立．

18．$f(n)=(3+(-1)^{n+1})/4$，或$f(n)=(n+1-2[n/2])/2$.

19．788; 210998.

21．(a) $533=13\cdot 41$; (b) $1073=29\cdot 37$.

22．(a) $170833=412^2+33^2=407^2+72^2=393^2+128^2=348^2+223^2=13\cdot 17\cdot 773$;

(b) $182410=427^2+9^2=423^2+59^2=409^2+123^2=401^2+147^2=383^2+189^2=381^2+193^2=347^2+249^2=303^2+301^2=2\cdot 5\cdot 17\cdot 29\cdot 37$.

25．其边数为下列各数的正多边形：3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34.

26．$x^2+(x+1)^2=(x(x+1)+1)^2-(x(x+1))^2$.

28．一般地，有$x^2+(1-x)=x+(1-x)^2$.

29．(a) 例如，$x=y=2^{1/4}$，$z=2^{1/2}$;

(b) 若$(a/b)^4+(c/d)^4=(r/s)^4$，则$(ads)^4+(bcs)^4=(bdr)^4$，这是不可能的．

30．当且仅当$b/c=a/(a^2-1)$时，有$(a+b/c)^{1/2}=a(b/c)^{1/2}$．所有形为$a+a/(a^2-1)$的数与$5+5/24$有相同的性质．

32．不是．它既非有限小数，又非循环小数．

33．(b) $(b-1)|(n-m)$.

35．(a) $p=5$; (b) 一个数也没有．

37．若$a+b\neq 0$，则x^2是无理数；若$a=-b$，则$x^2=a^2+b^2$是有理数．

39．7年前借了137元，利率为7%.

40．(b) 不成立：$111=3\cdot 37$.

42. 这些数都不能写为两个平方数之和.

45. (c) $f(2^n p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = (e_1+1)(e_2+1)\cdots(e_k+1)$.

50. (a) 1, 3, 5, 8, 15, 24, 40, 120; 1, 5, 8, 9, 40, 45, 72, 360;

(b) 可写为不同素数乘积的整数;

(c) 2^k;

(d) 在 10^{12} 以下的这种数只有 6, 60, 90.

56. (c) 例如, 18, 20, 24.

58. (b) 2, 以及与 1 同余(mod 4)的素数.

59. (d) $a=r^2+s^2$, $b=r^2-s^2$;

(e) a 和 b 是平方数, 比方说, $a=t^2$, $b=u^2$.

60. 6^2, 35^2, 204^2, 1189^2.

63. 若 $n\equiv 2 \pmod 4$, 则不可能有 $n=x^2-y^2$.

65. 最小的解为 $m=14$, $n=20$.

69. (a)

n	2	3	4	5	6	7	8	9	10	11	12
$f(n)$	2	3	4	5	3	7	6	6	5	11	4

n	13	14	15	16	17	18	19	20
$f(n)$	13	7	5	8	17	6	19	5.

70. 其末位数为 3.

71. 例如, $2^2+5^2+8^2+\cdots+23^2+26^2=48^2$.

72. (a) 9,876,543,210; (b) 98,763,210;

(c) 4,312; (d) 987,652,413.

74. 2^k, 其中 k 为 n 的正素因子个数.

75. (a) $4n^2-3n+1$; (b) $4n^2-2n+1$; (c) $4n^2+n+1$;

(d) $(n, -n)$; (e) $(-n+1, n)$; (f) $(9, 16)$.

77. (a) $m=4n(n+1)$; (b) 能.

78. 不对. 例如, 取 $n=4$, $m=3$.

79. 若 $(a, m)=d$, 则 $a, 2a, \cdots, ma$ 的最小剩余(mod m)中共含有 m/d 个数, 每个数重复了 d 次.

80. $P_n\equiv 3 \pmod 3$. 顺便指出, 当 $n=1, 2, 3, 4, 5$ 时, P_n 是素数, 但 $P_6=59\cdot 509$, 因此我们又否定了一个关于素数的公式.

81. 1, 2, 3, 5, 7, 11.

83．对．利用公式 $1^3+2^3+\cdots+n^3=(n(n+1)/2)^2$，可以证明，对所有 k，有 $2^{2k-2}(2^{2k-1}-1)=1^3+3^3+\cdots+(2^k-1)^3$．

84．若 $n=d_0+d_1\cdot 10+d_2\cdot 10^2+\cdots$，其中，$0\leqslant d_i\leqslant 9$，则当且仅当 $37\mid(d_0d_1d_2)+(d_3d_4d_5)+\cdots$ 时，有 $37\mid n$．

85．(a) $x=3t,\ y=5t,\ z=7t$，其中 t 为任意非零整数；

(b) 若 $k\not\equiv 2(\mathrm{mod}\,3)$，则 $x=3t,\ y=(k+4)t,\ z=(2k+5)t$；若 $k\equiv 2(\mathrm{mod}\,3)$，则 $x=t,\ y=(k+4)t/3,\ z=(2k+5)t/3$，其中 t 为非零整数．

86．$x=(a+b)/2,\ y=(a-b)/2$．

88．当 $r>1,\ n<180,000$ 时，此方程有解的唯一情况是：$18^2+18+1=7^3$．

91．(b) 不是：$2^6\equiv 2(\mathrm{mod}\,31)$．

93．(b) 必要条件为：-1 是一个二次剩余 $(\mathrm{mod}\,2k)$．

94．(b) 有：1806；(c) 没有了．

95．6 元．这一令人奇怪的问题是以下列事实为根据的：一个平方数的十位数若是奇数，则它的个位数必为 6．查看一下表 B 即可注意到这一点．要证明它，只须将各种情况罗列出来就可以了．

99．此方程的解为：

x	10	10	14	14	17	17	21	21	31	36	44	105
y	6	35	7	34	7	34	6	35	41	45	52	111.

103．(b) $r=78,\ s=5$，可得 $x=625,\ x^2=390625$．

附录一

2．$t_n=n(n+1)/2$．

5．$1^3+3^3+\cdots+(2k-1)^3=k^2(2k^2-1)$．

9．$(n+1)(6n^2+9n+2)/2$．

11．这种公式有无限多个，其中一个公式为：

$$f(n)=17(n-1)(n-2)(n-3)(n-4)/24.$$

12．不是．对所有 n，有 $8t_n+1=(2n+1)^2$．

附录二

1．(a) 112；(b) 1；(c) 2；(d) 27；(e) 34；(f) 328．

2. (a) $\sum_{i=0}^{6}(2i+1)^2$; (b) $\sum_{j=n}^{2n}1/j$; (c) $\sum_{k=0}^{n}a_kx^k$;

(d) $\sum_{t=0}^{r}u_{r-t}v_{n-r+t}$. 上述各式还可以有其它写法.

3. 易证(a)和(b)是成立的; (c)不成立: 可举出无限多个反例来说明这一点,例如,取 $a_k=b_k=1(k=1, 2, \cdots, n)$.

4. (a) $3^{1/2}$; (b) 1; (c) 8640; (d) 42; (e) 46.

5. (a) 40320; (b) 70; (c) 792.

7. (a) $x^6+12x^5+60x^4+160x^3+240x^2+192x+64$;

(b) $1-7a+21a^2-35a^3+35a^4-21a^5+7a^6-a^7$.

8. (a) $(x+3)^3$; (b) $(x-1)^n$.

9. 1, 2, 3, 5.

10. (a) 否; (b) 否.

11. $\|x\|=[x+1/2]$.

12. 0 和 -1.

13. (a) p^2-p; (b) $n-[n/p]$.

14. 19.

21. $[y]-[x]$.

附录三

1. (a) 68, 175; (b) 138, 487;

(c) 23, 105, 151, 223.

2. 无解.

3. (a) 4; (b) 6; (c) 4.

4. (a) 33, 117, 183, 267, 333, 417, 483, 567, 633, 717, 783, 867;

(b) 33, 217, 283, 467, 533, 717, 783, 967;

(c) 33, 517, 583, 1067.

5. 20.

7. 0, 1, 2, 4, 8.

8. $3^{e-1}-r$ 和 3^e-r 满足 $x^3\equiv -a(\mathrm{mod}\ p)$.

9. (a) 13; (b) 4, 13, 22.

参考文献

Oystein Ore, Number Theory and Its History, New York: McGraw-Hill, 1948.

B. W. Jones, The Theory of Numbers, New York: Holt, 1955.

J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, New York: McGraw-Hill, 1939.

Harriet Griffin, Elementary Theory of Numbers, New York: McGraw-Hill, 1954.

W. J. LeVeque, Topics in Number Theory (vol. 1), Reading, Mass.: Addison-Wesley, 1956.

van Niven and H. S. Zukerman, An Introduction to the Theory of Numbers, New York: Wiley, second edition, 1966.

Trygve Nagell, Introduction to Number Theory, Bronx, N. Y.: Chelsea, second edition, 1964.

G. H. Hardy and E. M. Wright, The Theory of Numbers, New York: Oxford Univ. Press, fourth edition, 1960.

G. H. Hardy, A Mathematician's Apology, New York: Cambridge Univ. Press, revised edition, 1967.

Waclaw Sierpinski, Elementary Theory of Numbers, New York: Hafner. 1964.

Daniel Shanks, Solved and Unsolved Problems in Number Theory, New York: Spartan, 1962.

P. J. Davis, The Lore of Large Numbers, New York: Random House, 1961.

Ivan Niven, Numbers, New York: Random House, 1961.

A. H. Beiler, Recreations in the Theory of Numbers, New York: Dover, 1964.

Tobias Dantzig, Number, New York: Macmillan, fourth edition, 1967.

L. E. Dickson, History of the Theory of Numbers (3 vols.), Bronx, N. Y.: Chelsea (reprint of the 1919 edition).

D. N. Lehmer, Factor Table for the First Ten Millions, New York: Hafner (*reprint of the 1909 edition*).

Waclaw Sierpinski, Pythagorean Triangles, New York: Academic Press, 1962.

A. O. Gelfond, The Solution of Equations in Intergers, San Francisco: W. H. Freeman and Company, 1961.

Ivan Niven, Irrational Numbers, New York: Wiley, 1956.

Harry Pollard, The Theory of Algebraic Numbers, New York: Wiley, 1950.

[General Information]
书名=基础数论
作者=()杜德利(U.Dudley)著
页数=285
SS号=10069053
出版日期=

目录
正文